DVTEL INC.
65 Challenger Road
Ridgefield Park, NJ 07660

dvtel·ioi
thermal by DRS Technologies

CT-5322F/CT-5642F
Fixed Thermal
Analytic IP Camera
User and Installation Guide

The contents of this guide may not be reproduced or reprinted in whole or in part without the express written permission of DVTEL, Inc.

dvtel® Now you can.

Ver. A4 October 11, 2015

Table of Contents

1 Document Information v
2 Introduction 1
2.1 Features 2
2.2 Items Included in the Package 3
2.3 Hardware Description 4
2.3.1 Connector Panel 4
3 Camera Installation and Mounting 6
3.1 Preparation 6
3.2 Items Required for Installation That Are Not Supplied 6
3.3 Attach the Base Mount to the Camera 7
3.4 Connecting the Camera Cables 7
3.5 Mounting the Camera 11
4 Connecting the Camera to a DVR 13
5 System Requirements 15
6 Discovering the Camera on the Network 16
7 Using the Web Interface 19
7.1 View Screen 20
7.2 Analytics 22
7.2.1 Configuring Depth Settings 23
7.2.2 Rules 29
7.2.3 Responses 31
7.2.4 Sched. Actions (Scheduled Actions) 36
7.2.5 On Screen Display 37
7.2.6 Analytic Firmware 38
7.2.7 Backup & Restore 39
7.3 Video Storage 40
7.4 Maintenance 41
7.4.1 System Status 41
7.4.2 Restart Camera 42
7.4.3 Restore Factory Defaults 42
7.4.4 Format Local Storage 43
7.4.5 System Update 44
7.4.6 Camera Functions 45
7.5 Setup 47
7.5.1 Configuring Network Settings 47

7.5.2 Configuring Account Settings 53
7.5.3 Configuring Camera Settings 53
7.6 Log Out 57
Appendix 59
A.1. Technical Specifications 60
A.2. Accessing a Remote Unit over the Web 62
A.3. CT-5322F/CT-5642F Mounting Accessories 64
A.4. Troubleshooting 70
A.5. Acronyms and Abbreviations 73
Contacting DVTEL 74

List of Figures

Figure 1: CT-5322F/CT-5642F Camera 1
Figure 2: CT-5322F/CT-5642F Connectivity 1
Figure 3: Package Contents 3
Figure 4: Connector Panel 4
Figure 5: Recommended Tools 7
Figure 6: Attaching the Base Mount 7
Figure 7: Cordgrip Parts 8
Figure 8: Cables Inserted through Locking Nut 8
Figure 9: Rubber Grommet 8
Figure 10: Wires Inserted through Rubber Grommet 8
Figure 11: Rubber Grommet Inserted into Cordgrip 9
Figure 12: Assembling Sealing Nut 9
Figure 13: Tightening the Locking Nut 9
Figure 14: Power Wires with Ferrite 9
Figure 16: Camera with Ferrites Installed for Power Supply 10
Figure 16: Back Cover and White Desiccant 10
Figure 17: Covering the Connector Panel 11
Figure 18: Solar Shroud and Stem Bumpers 11
Figure 19: Fully Assembled Camera 11
Figure 20: Login Window 17
Figure 21: ActiveX Installation Window 17
Figure 22: Render.cab Plug-in Dialog Box 17
Figure 23: Windows Restart Dialog Box 17
Figure 24: Home Page with Thermal Image 18
Figure 25: Web Interface with Callouts 19
Figure 26: Analytics > Depth Screen 23
Figure 27: Analytics > Depth Control Panel 25
Figure 28: Analytics > Depth > Step 1: Ground & Height Tab 25
Figure 29: Analytics > Depth > Step 2: Camera & Horizon Tab 26
Figure 30: Analytics > Depth > Step 3: Advanced Depth Regions Tab 27
Figure 31: Analytics > Depth > Step 4: Verification Tab 28
Figure 32: Analytics > Rules Screen 29
Figure 33: Analytics > Rules > Basic Attributes Tab 29
Figure 34: Analytics > Rules > Advanced Attributes Tab 30
Figure 35: Analytics > Responses Screen 31
Figure 36: Triggering Event Tab 31
Figure 37: Actions Tab 33
Figure 38: Schedule Tab 35
Figure 39: Sched. Actions > Actions Tab 36
Figure 40: Sched. Actions > Schedule Tab 37
Figure 41: Analytics > On Screen Display Screen 37
Figure 42: Analytics > Firmware Screen 38
Figure 43: Analytics > Backup & Restore Screen 39
Figure 44: Video Storage Screen 40
Figure 45: Video Storage Popup Viewer 40
Figure 46: System Status Screen 41

Figure 47: Restart Camera Screen 42
Figure 48: Restore Factory Defaults Screen 42
Figure 49: Format Local Storage Screen 43
Figure 50: System Update Screen 44
Figure 51: Heater Control Screen 45
Figure 52: Auto Calibration Interval Screen 45
Figure 53: Constant Recording Screen 46
Figure 54: Log Screen 46
Figure 55: Copyright Screen 47
Figure 56: TCP/IP Settings Screen 48
Figure 57: FTP Server Screen 49
Figure 58: Ping Target Screen 50
Figure 59: 802.1X Screen 51
Figure 60: Zero Network Configuration Screen 52
Figure 61: Accounts Screen 53
Figure 62: Date and Time Screen 54
Figure 63: Video Streaming Screen 55
Figure 64: Video Settings Screen 56
Figure 65: Analog Video Output Screen 57
Figure 66: Remote Access System 62

1 Document Information

Document Conventions	*Conventions relatives au document*
WARNING and CAUTION notes are distributed throughout this document, whenever applicable, to alert you of potentially hazardous situations. These may be hazards associated with a task or a procedure you are carrying out or are about to carry out. The following document conventions are used throughout this manual:	*Les remarques AVERTISSEMENT et ATTENTION sont réparties dans l'ensemble du document, en fonction des besoins, afin de vous avertir des situations potentiellement dangereuses. Il peut s'agir de risques associés à une tâche ou à une procédure que vous effectuez ou êtes sur le point d'effectuer.* *Les conventions suivantes sont utilisées dans l'ensemble du document:*

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

***Avertissement** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de blessure ou de mort.*

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

***Attention** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de dommages permanents pour l'équipement et/ou de perte de données.*

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

*Une **Remarque** est une information utile permettant d'éviter certains problèmes, d'effectuer une installation correcte ou de mieux comprendre les produits et l'installation.*

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of DVTEL products.

*Un **Conseil** correspond à une information et aux bonnes pratiques utiles ou apportant un avantage supplémentaire pour l'installation et l'utilisation des produits DVTEL.*

Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for:

- Physically connecting the ioi Thermal CT-5322F/CT-5642F fixed analytic IP camera
- Configuring setup parameters via the unit's web interface
- Operating the unit

Note:

This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Remarque:

Ce document est destiné aux utilisateurs techniciens qui possèdent des connaissances de base des équipements vidéo/caméras de télésurveillance et des connexions aux réseaux LAN/WAN.

Warning:

Installation must follow safety, standards, and electrical codes as well as the laws that apply where the units are being installed.

Avertissement:

L'installation doit respecter les consignes de sécurité, les normes et les codes électriques, ainsi que la législation en vigueur sur le lieu d'implantation des unités.

Proprietary Rights and Non-Disclosure

This manual is delivered subject to the following restrictions and conditions:

- This document contains proprietary information belonging to DVTEL, Inc. This information is supplied solely for the purpose of assisting explicitly the licensee of the DVTEL units.
- No part of this document contents may be used for any other purpose, disclosed to any third party or reproduced by any means, electronic or mechanical, without the express prior written permission of DVTEL, Inc.

Legal and Environmental Information

This product contains technology controlled under the U.S. Export Administration Regulations (EAR). Diversion contrary to U.S. law is prohibited. This product has been tested and found to comply with the limits of FCC Class A Part 15 Subpart B and CES-003. This product complies with the European RoHS directive.

Trademarks and Copyrights

DVTEL, the DVTEL logo, ioi, the ioi logo, ioi analytics, ioibox, ioicam, ioi HD, ioi IP, ioi Thermal, and Site Viewer are trademarks of DVTEL, Inc. Products and trademarks mentioned herein are for identification purposes only and may be registered trademarks of their respective companies. DVTEL, Inc. makes no representations whatsoever about any other products or trademarks mentioned in the manual. This manual and its contents herein are owned by DVTEL, Inc. © DVTEL, Inc. 2015. All rights reserved.

Disclaimer

Users of DVTEL products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements.

DVTEL, Inc. and its agents make no guarantees or warranties to the suitability for the users' intended use. DVTEL, Inc. accepts no responsibility for improper use or incomplete security and safety measures.

Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve DVTEL, Inc. and its agents from any resulting liability.

Specifications and information in this guide are subject to change without notice.

Avis de non-responsabilité

Il incombe aux utilisateurs des produits DVTEL de vérifier que ces produits sont adaptés et d'étudier le rôle des capacités et limites de détection du produit appliqués aux exigences uniques de leur site.

DVTEL, Inc. et ses agents ne garantissent d'aucune façon que les produits sont adaptés à l'usage auquel l'utilisateur les destine. DVTEL, Inc. ne pourra être tenu pour responsable en cas de mauvaise utilisation ou de mise en place de mesures de sécurité insuffisantes.

Le non respect de tout ou partie des procédures recommandées ou des messages d'AVERTISSEMENT ou d'ATTENTION de la part de l'installateur, du propriétaire ou de l'utilisateur dégagera DVTEL, Inc. et ses agents de toute responsabilité en résultant.

Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Précautions et avertissements d'ordre général

Cette section contient des informations indiquant qu'une procédure ou condition présente des risques potentiels.

CONSERVEZ *TOUTES LES INSTRUCTIONS DE SÉCURITÉ ET D'UTILISATION POUR POUVOIR VOUS Y RÉFÉRER ULTÉRIEUREMENT.*

Bien que l'unité soit conçue et fabriquée conformément à toutes les normes de sécurité en vigueur, l'installation de cet équipement présente certains risques.

Afin de garantir la sécurité et de réduire les risques de blessure ou de dommages, veuillez respecter les consignes suivantes:

Warning:

1. The unit's cover is an essential part of the product. Do not open or remove it.
2. Never operate the unit without the cover in place. Operating the unit without the cover poses a risk of fire and shock hazards.
3. Do not disassemble the unit or remove screws. There are no user serviceable parts inside the unit.
4. Only qualified trained personnel should service and repair this equipment.
5. Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

Avertissement:

1. *Le cache de l'unité est une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.*
2. *N'utilisez jamais l'unité sans que le cache soit en place. L'utilisation de l'unité sans cache présente un risque d'incendie et de choc électrique.*
3. *Ne démontez pas l'unité et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.*
4. *Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.*
5. *Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.*

Caution:

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range specified for the product -40° to 60°C (-40° to 140°F) with no more than 95% non-condensing humidity.

Attention:

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage de température spécifiée pour le produit (0° à 60°C/32° à 140°F), sans condensation d'humidité supérieur à 95%.

Electrical Safety Notice and Warnings

Warning:

1. Read the installation instructions before you connect the unit to a power source.
2. Electrical safety should always be observed. All electrical connections must be performed by a certified electrician.
3. If you use a power supply, be sure to protect against static electricity, ground faults and power surges.
4. If you use an extension cord with this system, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.
5. To avoid possible shock hazards or damaging the unit, ensure that the positive and negative of the power leads are properly connected to the terminal block connector before plugging it into the unit or turning on the power source.
6. In the following situations, the electric power should be turned off immediately and appropriate repairs, replacements or remedies should be taken if:
   - The power line or plug is damaged, frayed or shows heavy wear.
   - The unit has been physically crushed or deformed.
   - The unit has been exposed to water.
   - The unit has been exposed to, or shows signs of damage from, fire, intense heat, heavy smoke, fumes, or vapors.
   - Electrical connections of the unit become abnormally hot or generate smoke.
   - The unit has been dropped, damaged or shows signs of loose internal parts.
   - The unit does not operate properly.

Avis et avertissements relatifs à la sécurité électrique

Avertissement:

1. *Lisez les instructions d'installation avant de brancher l'unité à une source d'alimentation électrique.*
2. *Les consignes de sécurité électrique doivent toujours être respectées. Toutes les connexions électriques doivent être effectuées par un électricien qualifié.*
3. *Si vous utilisez une alimentation, assurez-vous de protéger l'unité contre l'électricité statique, les défauts de mise à la terre et les surtensions.*
4. *Si vous utilisez une rallonge avec ce système, assurez-vous que l'ampérage total des produits branchés sur la rallonge ne dépasse pas l'ampérage nominal de celle-ci.*
5. *Pour éviter tout risque de choc électrique ou d'endommager l'unité, assurez-vous que les bornes plus et moins de l'alimentation sont correctement raccordées au connecteur du bloc de jonction avant de le brancher sur l'unité ou d'activer la source d'alimentation.*
6. *Dans les situations suivantes, l'alimentation électrique doit être coupée immédiatement, et les réparations, remplacements ou solutions suivants doivent être effectués si :*
   - *Le cordon d'alimentation ou la prise (le cas échéant) est endommagé, effiloché ou très usé.*
   - *L'unité a subi un choc ou a été déformée.*
   - *L'unité a été exposée à de l'eau.*
   - *L'unité a été exposée à, ou montre des signes de dégâts par le feu, une chaleur intense, une fumée épaisse, des émanations ou des vapeurs.*
   - *Les connexions électriques chauffent de façon anormale ou produisent de la fumée.*
   - *L'unité est tombée, a été endommagée, ou certaines pièces internes semblent détachées.*
   - *L'unité ne fonctionne pas correctement.*

Camera Warnings

Warning:

1. Be sure not to expose the camera head to strong sunlight, which could cause the camera to overheat.
2. This product must be connected to a PoE+ IEEE 802.3at-compliant power source, or a UL listed Class 2 power supply rated 12-24 VDC or 24 VAC, minimum 20W.
3. Operating the camera at voltage levels outside the specified range may result in permanent damage to the unit and void the product warranty.
4. The camera electronics and electronic interfaces are sensitive to electrostatic discharge. Follow appropriate ESD procedures when handling the camera and during installation.
5. For PoE+ installations, we strongly recommend using STP cabling and an earth grounded end point to ensure proper ESD immunity. For installations powered by AC or DC, a properly earth grounded power source is strongly recommended. Any other installation method may leave the camera at risk and void the warranty.

Avertissements relatifs à la Caméra

Avertissement:

1. *Assurez-vous de ne pas exposer la tête de la caméra aux rayons de soleil intenses qui pourraient surchauffer la caméra.*
2. *Ce produit doit être connecté à une source d'alimentation PoE+ conforme à la norme IEEE 802.3at, ou à une alimentation UL de Classe 2 de 12-24 V CC ou 24 V AC, 20W minimum.*
3. *Toute opération de la caméra à des niveaux de tension n'étant pas compris dans la fourchette indiquée peut endommager l'unité de façon permanente et peut annuler la validité de la garantie du produit.*
4. *L'électronique et les interfaces électroniques de la caméra sont sensibles aux décharges électrostatiques. Suivez les procédures ESD adéquates lors de toute manipulation de la caméra et au cours de son installation.*
5. *Pour les installations PoE+, nous recommandons fortement d'utiliser des câbles STP et une liaison à la terre pour assurer l'immunité face aux décharges électrostatiques. Pour les installations alimentées par AC ou CC, une source d'alimentation reliée à la terre est fortement recommandée. Toute autre méthode d'installation peut comporter des risques pour la caméra et annuler la garantie.*

Minimizing EMI and RFI	*Minimisation des IEM et des IRF*
When wires run for a significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur. Strong EMI (e.g. lightning or radio transmitters) can destroy the units and can pose an electrical hazard by conducting power through lines and into the system. Poor quality or worn wiring can result in radio frequency interference (RFI). To minimize the effects of EMI and RFI, consult your reseller.	*Lorsque des câbles parcourent une distance importante dans un champ électromagnétique, des interférences électromagnétiques (IEM) peuvent se produire. D'importantes IEM (comme la foudre ou un émetteur radio) peuvent détruire les unités et présenter un risque électrique si elles se propagent sur les câbles et dans le système. Des câbles de mauvaise qualité ou usés peuvent provoquer des interférences radioélectriques (IRF). Pour minimiser les effets des IEM et des IRF, consultez votre revendeur.*

Site Preparation

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- **Ambient Environment Conditions:** Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that the unit is free from dust, dirt, smoke, particles, chemicals, smoke, water or water condensation, and exposure to EMI.
- **Accessibility:** The location used should allow easy access to unit connections and cables.
- **Safety:** Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations:** Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security:** The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security:** The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. The unit is intended for installation on the backbone of a trusted network.
- **Electrostatic Safeguards:** The unit as well as other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc) shall be properly grounded to prevent electrostatic discharge.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity.

2 Introduction

The ioi Thermal CT-5322F/CT-5642F are fixed-mount, fixed-focal length thermal cameras with built-in video analytics. The cameras provide real-time H.264 and MJPEG streaming video from their IP and analog video outputs.

Ioi Thermal analytic cameras deliver outstanding peformance. They offer enhanced detection, even of small objects from a distance, even in scenes where there are large or multiple objects and movement in up to 80% of the frame. The system can detect sophisticated intruders and enable the identification of people who are standing upright, running or walking, which reduces false alarms.

The cameras' video analytics provide alarms when they automatically detect specific events, such as region entrance, fence trespassing, tripwire crossover, which trigger an automatic notification. You can define the events and location in the video of the image that can be detected with user-customizable rules, positioning criteria, responses, and scheduled actions.

Figure 1: CT-5322F/CT-5642F Camera

The CT-5322F/CT-5642F uses an uncooled 320 x 240 resolution focal plane array (CT-5322F) or 640 x 480 resolution focal plane array (CT-5642F), with 17µm Vox thermal imaging technology. It detects infrared (heat) waves in the 8-14µm wavelength. The camera delivers superior thermal images in challenging environments, including in complete darkness, over water and in dark corners, where lighting constraints and weather conditions make threats difficult to detect. The camera is available in two versions: 9 FPS fixed frame rate or variable frame rate up to 30 FPS.

The camera simultaneously provides video output in two formats: analog video and compressed digital video over IP. It complies with IEEE 802.3at PoE+ standards, supporting video, camera control and power over a single, tamper-resistant Ethernet cable connection. It can be configured and installed easily in any existing security infrastructure via its web-based configuration.

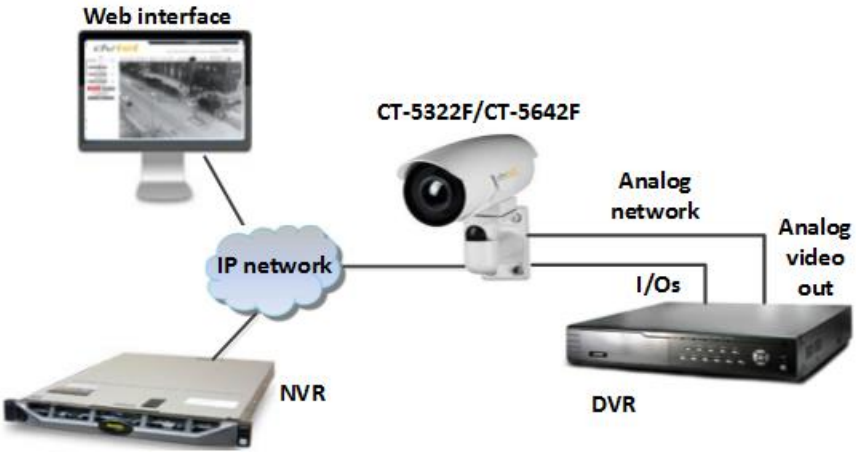


Figure 2: CT-5322F/CT-5642F Connectivity

The CT-5322F/CT-5642F is efficient, compact and lightweight, consumes less than 20 watts, and weighs less than 2.6 pounds (1.2 kg). When not being powered by an AC or DC supply, the camera requires an IEEE 802.3at PoE+ source.

Note:
IEEE 802.3af PoE is NOT supported.

The camera is sealed in an IP66 outdoor-rated enclosure, which makes it ideal for outdoor sureveillance of critical infrastructure such as airports, utility companies, and nuclear power plants.

The camera is available with these fully sealed, hard carbon-coated, athermalized fixed-focus lenses:

Series	Horizontal Field of View
CT-5322F	6°, 9°, 16°, 24°, or 40°
CT-5642F	12°, 18°, 25°, 37°, or 44°

This chapter includes the following sections:

- Items Included in the Package (page 3)
- Hardware Description (page 4)

2.1 Features

Following are key general features of the CT-5322F/CT-5642F camera:

- VGA and QVGA models
- 9 or 30 FPS models
- Wide range of lenses
- Advanced video analytics
- Superior intruder detection
- Customizable analytic rules and actions
- H.264 and MJPEG compression
- HTTP streaming MJPEG
- Uncooled Vanadium Oxide Microbolometer sensor
- SNMP v1/v2/v3 and SNMP traps
- PAL/NTSC analog video output (BNC connector)
- Built-in web application/ web server
- 3.5GB embedded flash memory storage available
- Store constant video and events
- Upload video files via FTP
- ONVIF and HTTP alarm notification
- Analytic detection event driven alarms
- Two alarm input driven events
- Relay output actions on alarm
- ONVIF Profile S support
- RTSP support
- User permissions according to role
- Supports PoE+/12VDC/ 24VAC
- Vandal-proof IP66 enclosure
- Built-in heater

The camera supports the following analytic functions:

- Analytic relay events
- Reduced false alarm rate
- Increased detection distance
- Intrusion detection
- Unattended baggage detection
- Object removal detection
- Stopped vehicle detection
- Loitering detection
- Camera tampering detection

2.2 Items Included in the Package

The unit package contains the following items:

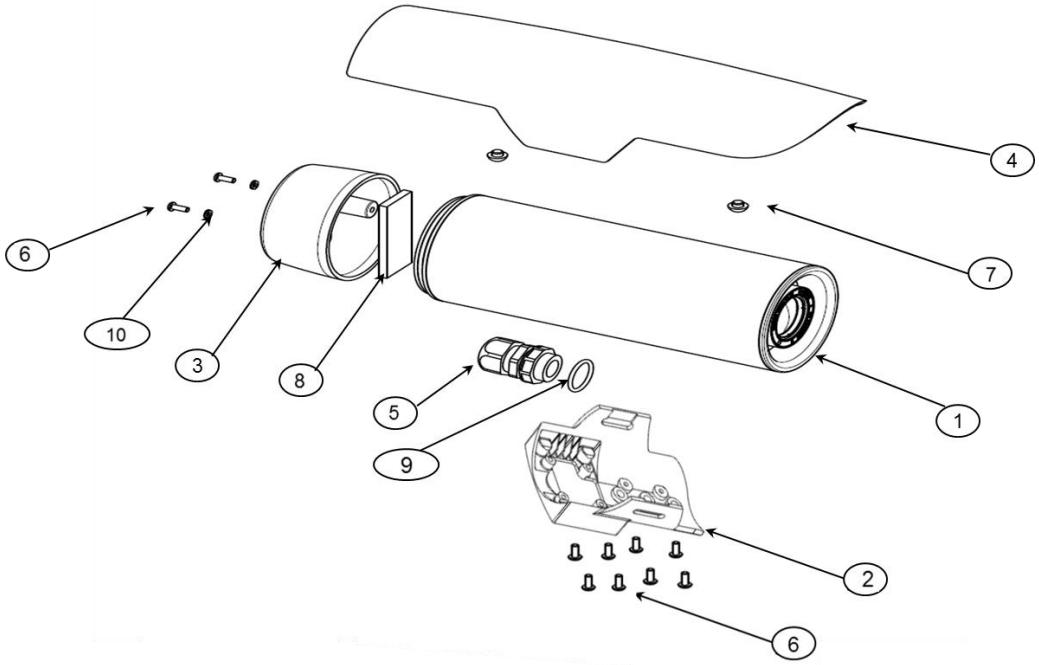
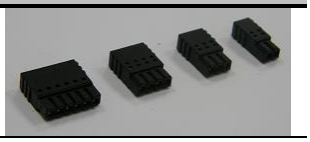


Figure 3: Package Contents

Item	QTY	Description
1	1	CT-5322F/CT-5642F Fixed Thermal Analytic IP Camera (including 90° BNC adapter attached to the back of the camera)
2	1	Base mount
3	1	Back cover
4	1	Solar shroud
5	1	Liquid tight cordgrip
6	8	#6 32 x 5/8” screws (plus spares)
7	3	Stem bumpers (including one spare)
8	1	White desiccant for installation
9	1	Rubber O-ring (shown as installed on cordgrip)
10	3	Sealing washers with gasket (including one spare)

In addition, the following items are included in the package:

QTY	Description	
1	Package of four terminal connectors: 6-pin for alarms and relay; 4-pin for audio; 3-pin for power and ground; and 2-pin for RS-485	
1	Locking Nut	
1	Quick Installation Guide	
2	Ferrites (for power and alarm leads)	

Note:

1. The camera can be powered from an IEEE 802.3at PoE+ source, from a 12-24 VDC source, or from a 24 VAC source, which should supply 20W.
2. IEEE 802.3af PoE is NOT supported.

Related Documentation:

- *ioi Thermal CT-5322F/CT-5642F Quick Installation Guide*
- *HTML Edition Units User's Guide*
- *DNA User Manual*

2.3 Hardware Description

This section describes the physical connections to the unit.

2.3.1 Connector Panel

The rear panel of the camera includes the following items:

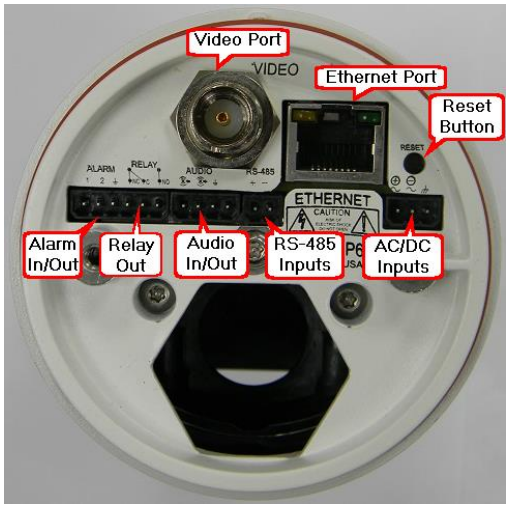


Figure 4: Connector Panel

Item	Description
Video Port	Connects the video coax cable between the camera and an analog DVR.
Ethernet Port	Connects the network cable between the camera and the network switch for network communication and powering the unit via PoE+. **Note:** IEEE 802.3af PoE is NOT supported.
10 Mbps LED on Ethernet Port	Off – LAN connection is not detected Solid amber – 10 Mbps LAN connection is detected Flashing amber – Data is being transmitted or received via the LAN connection
100 Mbps LED on Ethernet Port	Off – LAN connection is not detected Solid green – 100 Mbps LAN connection is detected Flashing green – Data is being transmitted or received via the LAN connection
Alarm In/Out	Connects two alarm inputs via the supplied 6-pin connector to the marked 1, 2, and ground pins. Each alarm input pin should also be connected to the ground pin, i.e., pin 1 + ground, or pin 2 + ground.
Relay Out	Connects the supplied 6-pin connector to the marked NC, C, and NO pins. The NC and NO pin should also be connected to the C pin. i.e., NC + C, or NO + C.
Audio In/Out	Not currently supported.
RS-485	Not currently supported.
Reset button	For resetting the camera to factory default settings. Insert a small, pointed object into the recess, press the button, and hold for at least 6 seconds.
AC/DC Pins	Connects a male 3-pin connector from an AC or DC power supply to the unit's **+** (positive), **–** (negative), and ground leads.

3 Camera Installation and Mounting

The physical installation of the camera is the first phase of making the unit operational. The goal is to physically place the unit, connect it to other devices in the system, establish IP network connectivity, and configure the camera for operation.

Caution:

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range specified for the product (-40° to 60°C/-40° to 140°F), with no more than 95% relative humidity, non-condensing).

Attention:

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la température est suffisante pour répondre aux temperatur de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage de température spécifiée pour le produit (-40° à 60°C/-40° à 140°F), sans condensation d'humidité supérieur à 95%).

3.1 Preparation

Read the instructions in this chapter thoroughly before installing the camera. Following are additional considerations for outdoor installation:

- Always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- To minimize the effects of EMI (electromagnetic interference) and RFI (radio frequency interference), consult your reseller.

3.2 Items Required for Installation That Are Not Supplied

The following items are required for installation, but are not included in the package:

- Power source (PoE+ switch, 12-24VDC or 24VAC power supply)
- Shielded Twisted Pair (STP) cable if using a PoE+ switch
- Cat 5 Ethernet cable for network connection without a PoE+ switch
- Tripod or mounting bracket for mounting the camera
- One #2 Phillips head screwdriver
- One open-end, 1-inch (25.4mm) wrench or adjustable wrench
- One 6-inch (152mm) scale or ruler
- Electric or manual torque screwdriver set to 10 inch-pounds (1.23 newton meters)
- Hex wrench
- RJ45 connector
- RJ45 crimping tool
- Coax cable
- Coax cable cutter/stripper
- BNC connector

- BNC crimping tool

Figure 5: Recommended Tools

3.3 Attach the Base Mount to the Camera

To attach the base mount to the camera

1. Screw the base mount into the camera body with eight #6 screws.

Figure 6: Attaching the Base Mount

2. Using the electric screwdriver, tighten the fasteners to about 8 inch-pounds (0.904 newton meters) of torque.
3. Using the electric screwdriver and the Torx T10 security bit, tighten the fasteners to about 10 in-lbs. (1.23 newton meters) of torque.

3.4 Connecting the Camera Cables

In order to connect the camera to the network, take the analog video cable, network cable, power supply leads (if an AC or DC supply is used), and alarm, relay, and RS-485 wiring (if used) from the wall at the installation site.

In order to connect the wires to the connectors on the camera's connector panel, they must be wired through the supplied cordgrip. Wires must be fed from the wall through the camera's mounting assembly, through the opening on the underside of the camera, through the camera body, and out of the opening on the camera's connector panel. The wires then must be attached to connectors before attaching them to the connector panel.

To prepare the camera cabling

1. Disconnect power from any previously installed cables.
2. Remove the cordgrip parts from the package.

Figure 7: Cordgrip Parts

3. Feed the wires through the locking nut, then through the camera body and out of the opening on connector panel.

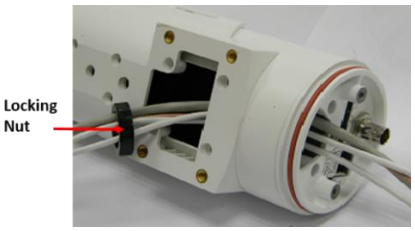


Figure 8: Cables Inserted through Locking Nut

4. Feed the wires through the cordgrip body as seen in the picture above.
5. Place the orange O-ring over the cordgrip and feed the wires through the cordgrip body and sealing nut as seen in Figure 10.
6. Insert the Ethernet cable through the center opening of the rubber grommet. Then insert the other wires through the small holes in the rubber. The wires should be spaced several holes apart. Nineteen (19) AWG is recommended for the power leads. Twenty (20) AWG is recommended for all wires other than the Ethernet and video cables. The flat side of the grommet should be on the inside of the cordgrip.

Figure 9: Rubber Grommet

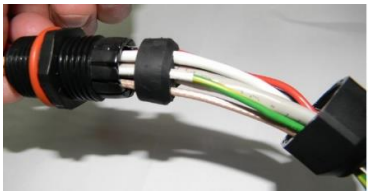


Figure 10: Wires Inserted through Rubber Grommet

7. If needed, use a #2 Phillips head screwdriver to widen the hole in the center of the rubber grommet (Figure 9).
8. If needed, pierce the smaller holes on the outer perimeter of the rubber grommet for the video cable, AC/DC supply wiring, audio, alarm, relay, and RS-485 leads.
9. Measure about 4-1/2” (114mm) of cable from the end of all wires to the rubber grommet.

10. Push the rubber grommet into the cordgrip body so that the grommet is flush with the slotted side of the body and the flat side of the sealing nut is facing it.

Figure 11: Rubber Grommet Inserted into Cordgrip

11. Insert the wires through the sealing nut and screw the nut clockwise so that it is closes tightly on the cordgrip body. Use the hex wrench to tighten the nut to 50-55 inch-pounds (5.65-6.215 newton meters) of torque so that the cordgrip is securely fastened.

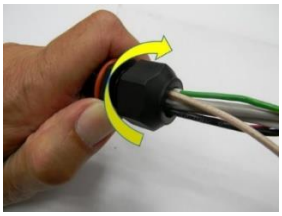


Figure 12: Assembling Sealing Nut

12. Insert the assembled cordgrip into the opening on the connector panel. The side including the exposed screw thread and rubber O-ring should be inserted first.
13. Hand-tighten the locking nut inside the camera body.

Figure 13: Tightening the Locking Nut

14. Use the hex wrench to tighten the nut to approximately 8 in-lbs. (0.9 newton meters) of torque so that the cordgrip is securely fastened.
15. Using a striping tool, attach an RJ45 connector (not supplied) to the Ethernet cable and an RJ179BU male BNC crimp connector (not supplied) to the video cable. Crimp the wires onto the connectors.
16. If the camera is connected to an alarm or a 12 or 24 volt power supply, it is necessary to insert the wires through the supplied ferrites in order to comply with EMI emission standards.

Figure 14: Power Wires with Ferrite

17. Attach the supplied plugs to the wires. Crimp the wires onto the connectors.
18. If using a power supply, connect the 3-pin male terminal block connector from the power supply to the AC/DC power input.

19. Insert the connectors and plugs into the connector panel.

Figure 15: Camera with Ferrites Installed for Power Supply

Note:

If you use a PoE+ switch, in order to ensure a proper earth ground between the camera and the switch, we strongly recommend using Shielded Twisted Pair (STP) cabling. Installations of ioi Thermal cameras with STP cabling and a properly earth grounded PoE+ switch are tested to comply with industry immunity standards for electrostatic discharge (ESD). Any other installation method may leave the camera at risk and void the warranty.

20. Reconnect power to the cables.
21. Check for a steady LED indication on the Ethernet cable RJ45 connector to confirm connection to the IP network. The status LED indicators are:
    - LED 1: Steady green for 10MB connection or flashing green for activity.
    - LED 2: Steady amber for 100MB connection or flashing amber for activity.
22. Insert the supplied white desiccant inside the back cover.

Figure 16: Back Cover and White Desiccant

23. Close the rear cover over the assembled connector panel by aligning the notch on the cover with the notch in the camera body. If necessary, reinsert excess cable into the body of the camera.

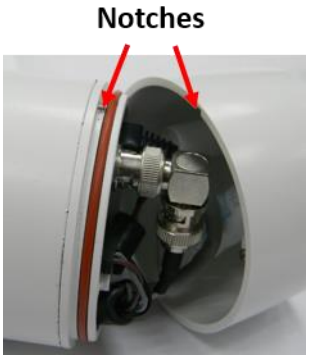


Figure 17: Covering the Connector Panel

24. Attach the back cover to the camera. Screws are pre-installed in the back cover.
25. Tighten the two fasteners to approximately 8 in-lbs. (0.904 newton meters) of torque.
26. Assemble the two rubber stem bumpers onto the two detents in the concave surface of the solar shroud.

Figure 18: Solar Shroud and Stem Bumpers

27. Snap the solar shroud over the camera body. The camera is ready for mounting.

Figure 19: Fully Assembled Camera

3.5 Mounting the Camera

The camera can be mounted on a tripod or on a base mount or four-hole bracket.

- For tripod mounting, use the tripod adapter, which is available as an accessory.
- For base mounting, install the camera base mount on a standard flat side bracket (not provided) using the supplied #6 32 x 5/8” screws.

See the Appendix (page 62) for a full list of mounting accessories.

4 Connecting the Camera to a DVR

The analog video output (composite video) contains the video from the camera combined with On-Screen Display (OSD) overlays such as detected objects, tracking boxes and trails, time stamp, alarm, camera status, and so on. These OSDs can be enabled and customized using the unit's embedded HTML user interface. The analog video output can be recorded on a digital video recorder (DVR). Analytic events can trigger the camera's I/O relay status to change, which triggers an event on the DVR. For more information, refer to the *HTML Edition Units User's Guide*.

5 System Requirements

To access the CT-5322F/CT-5642F Fixed Thermal Analytic IP camera via a web browser, ensure that your PC has the proper network connection and meets the system requirements described below.

Item	Camera Client Application System Requirements
Personal Computer	Intel® Pentium® M, 2.16 GHz or Intel® CoreTM2 Duo, 2.0 GHz 2GB RAM or better
Operating System	Windows 7, 8, or 8.1
Web Browser	Microsoft Internet Explorer 8, 9, 10, 11
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

6 Discovering the Camera on the Network

After installing the camera, the unit must be discovered on the network. After doing this, you can then configure camera settings and view live video from the camera's web Interface.

DVTEL recommends using the DVTEL Network Assistant (DNA) tool to discover the camera on the network. DNA is a user-friendly utility that is designed to easily discover and configure DVTEL edge devices on a network. The DNA tool has a simple user interface and does not require any installation. The software is provided as a single, standalone executable. It runs on any PC.

DNA provides a central location for listing all the DVTEL camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings. If the network settings are changed for some reason, a new search will relist the units. The units may then be configured via the web interface.

If DVTEL Latitude is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication. The camera must be made accessible for the network's addressing.

For detailed instructions about how to use DNA, see the *DNA User Manual*, which is included in the CD provided with the camera. You can also download the manual from the *Downloads* tab at http://www.dvtel.com/products-solutions/tools/.

Note:

Use a DHCP server to facilitate discovery of the unit's IP Address. Confirm that *Use DHCP* is checked in DNA's **Assign IP** dialog box.

By default, when the camera powers on, it attempts to obtain an IP address from a DHCP server in the network. If the camera cannot obtain an IP address through DHCP within a reasonable time, it will default to an IP address of 192.168.0.200 and a subnet mask of 255.255.255.0.

In the event that you do not have access to the DHCP server:

1. Set 192.168.0.11 as the IP address for the client PC.
2. Use the Windows Network tool to locate the camera and set the static IP address.

To discover devices using DNA

1. Download the DNA utility from the DVTEL Partner Portal, or copy the DNA utility from the CD included in the package.
2. Click the DNA icon and run the DNA utility (`DNA.exe`). DNA discovers all devices on the VLAN.
3. Assign IP address to the device.
4. Click the **Login** icon and enter login credentials for the devices.

5. Enter the unit's IP address in your browser (IE 8, 9 10, or 11). The **Login** window opens.

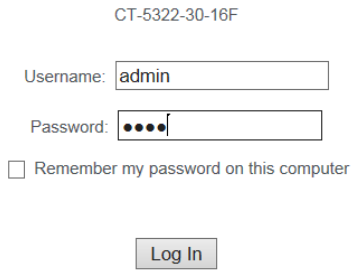


Figure 20: Login Window

6. Enter the unit's default user name ("admin") and password ("admin")

> **Note:**
>
> The username is case-sensitive.

7. Click **Log In**. A dialog box opens.

Figure 21: ActiveX Installation Window

8. Click **Click here** to install the ActiveX component. Installation can take up to 3 minutes. At the end of the process, an Internet Explorer dialog box opens.

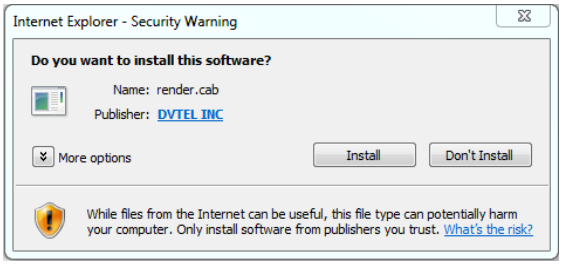


Figure 22: Render.cab Plug-in Dialog Box

9. Click **Install** on the Internet Explorer dialog box requesting to you to install the `render.cab` plug-in. Occasionally, after installing the plug-in, a Windows dialog box opens.

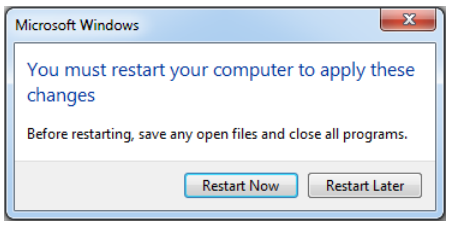


Figure 23: Windows Restart Dialog Box

10. Click **Restart Now** on the Windows dialog box to restart the computer. The computer restarts.
11. Open your browser and enter the camera's IP address. The **Login** window opens. See Figure 20: Login Window.
12. Enter the user credentials in the **Login** window. The camera's home page opens with a thermal image displayed in the **Live View** window.

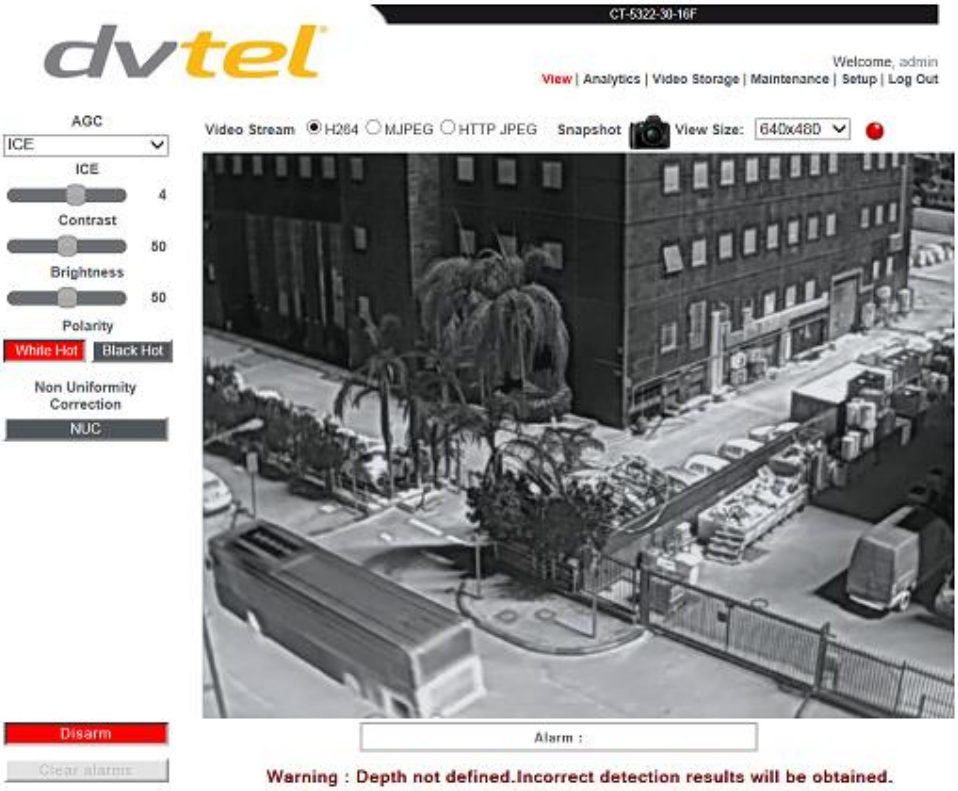


Figure 24: Home Page with Thermal Image

7 Using the Web Interface

The CT-5322F/CT-5642F web interface is used for monitoring live video and configuring the camera.

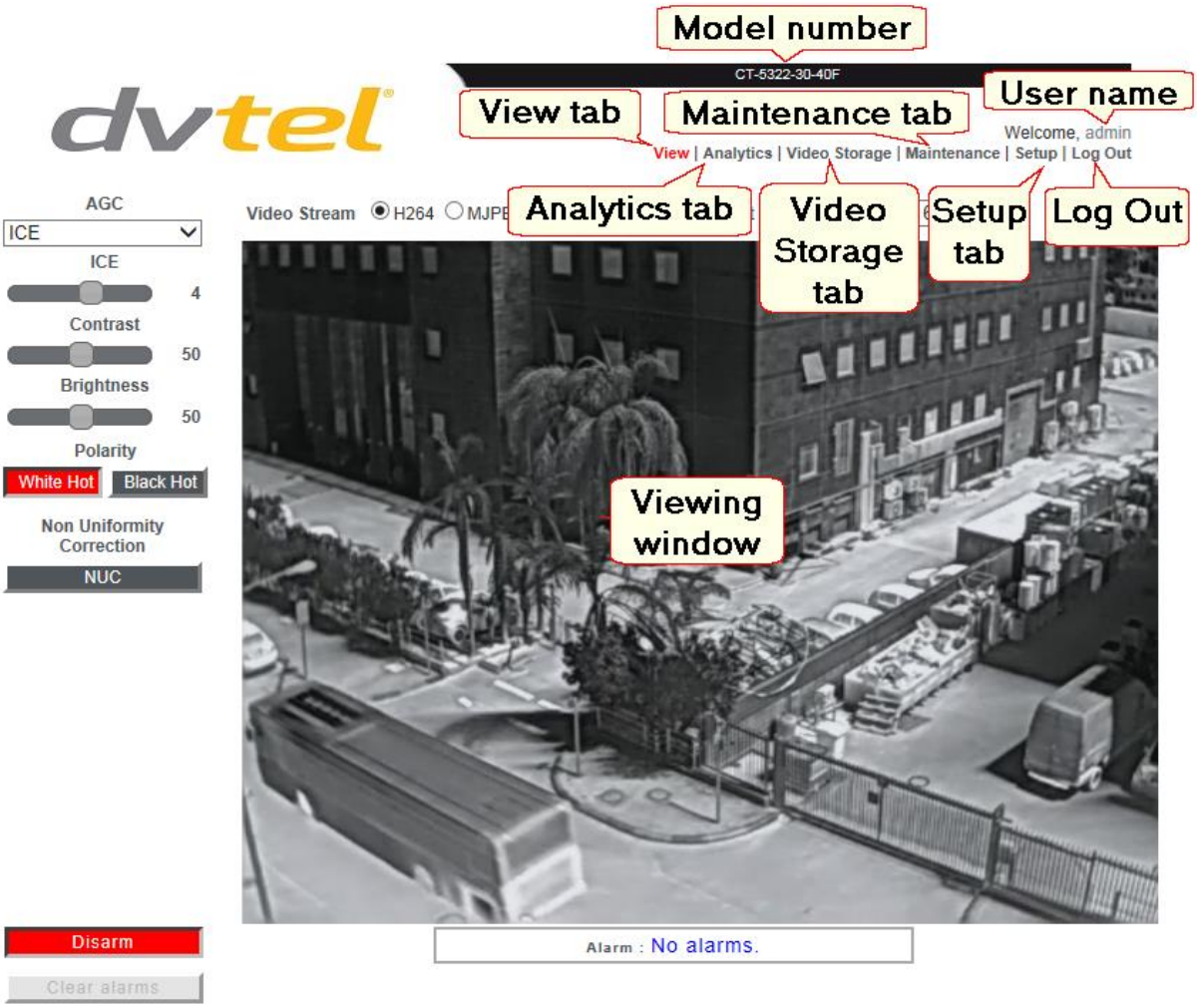


Figure 25: Web Interface with Callouts

The following tabs are accessible from the home page:

- View Screen (page 20)
- Analytics Screen (page 22)
- Video Storage Screen (page 40)
- Maintenance Screen (page 41)
- Setup Screen (page 47)

The web interface also displays the camera model number and the username. The **Log Out** link enables logging off the camera.

Access to the various screens is determined by the privileges assigned to the user. There are three user roles ("user classes"): Administrators, Operators, and Viewers:

- Administrators can access all of the IP camera menus, features and functions
- Operators have access to limited IP camera menus, features and functions
- Viewers can only view live video and access image controls

The user role (class) determines the access to the different menus and actions that can be performed from the unit's web interface. The following table details the privileges for each user role (class) by menu screen:

Screen	Description	Privilege
View	Live video and image controls	Administrator, Operator, Viewer (can only view the video stream)
Analytics	Configuration of analytic depth setings, rules, responses, scheduled actions, on-screen display, firmware version selection, and firmware/configuration backup and restore	Administrator
Video Storage	Recording and Storage of video and images	Administrator, Operator
Maintenance	System updates, camera reset, factory default, and camera functions	Administrator
Setup	IP network settings, user and account management and camera controls	Administrator

User privileges are configured from the **Setup > Accounts** screen. See Configuring Account Settings (page 53).

7.1 View Screen

The **View** screen is used to view live video and for configuring image controls. After logging in for the first time or loading a new firmware version, you must enable the ActiveX plug-in in order to view live video. See Discovering the Camera on the Network. All users have access to the **View** screen. See Figure 24: Home Page with Thermal Image.

Configure the following settings from the **View** screen from the menu above the **View** screen:

Item	Description
Video Stream	Select the video stream: H.264, MJPEG, or HTTP JPEG. You can select multiple video streams, which open in separate browser windows. HTTP JPEG is recommended for: ▪ Accessing a unit that is located behind a firewall at a remote site ▪ Transmitting video via HTTP over remote networks with low bandwidth ▪ Remote configuration of the unit over the web ▪ If you have difficulty viewing the video in H.264 **Note:** The ioi camera enables access to a camera that is not IP-enabled at a remote site over the Web. For more information about this capability, see Accessing a Remote Unit Behind a Firewall (page 62).
Snapshot	Click the icon to take a snapshot of the image.

Item	Description
View Size	Adjust the video viewing window to the following sizes: 160 x 120, 320 x 240, or 640 x 480 (default).
	The icon above the top-right corner of the image indicates whether constant **recording is** active (red dot) or inactive (gray dot).

Configure the following settings from the **View** screen from the sidebar:

Item	Description
AGC	Automatic Gain Control (AGC) adjusts the gain and level of the entire scene in real-time. From the drop-down menu, select a mode: ▪ *Freeze* – Turns off/freezes AGC at its current level. ▪ *Auto* – Provides an image with optimum average contrast and brightness ▪ *ICE* – Enhanced gain control/ Image Contrast Enhancement (ICE). In low-contrast indoor scenes it reduces detector noise and prevents the darkening of scenes when hot objects appear. In high-contrast scenes outdoor scenes, it amplifies detector noise and darkens the scenes when hot objects appear.
ICE	Move the slider to adjust the strength of the AGC settings. The range is from 0-7. The higher the number, the better the picture. The default setting is 4.
Contrast	Move the slider to adjust the contrast. The range is from 0-100. The higher the number, the higher the contrast. The default setting is 50.
Brightness	Move the slider to adjust the brightness. The range is from 0-100. The higher the number, the brighter the picture. The default setting is 50.
Polarity	Enables you to select how to display hot and cold pixels. Select one of the following settings: ▪ *White Hot* – Hot pixels are displayed as white and cold pixels are displayed as black. ▪ *Black Hot* – Hot pixels are displayed as black and cold pixels are displayed as white.
Non Uniformity Correction (NUC)	Normally, an NUC is performed automatically to compensate for temperature variations. Click this button to manually force a Non Uniformity Correction. The NUC interval can also be set using the maintenance/camera functions menu.
Arm/Disarm	Click this button to arm or disarm the camera. You must disarm the camera in order to configure the unit.
Clear Alarms	Click this button to clear alarms that you have set. The alarm status is indicated under the viewing window.

7.2 Analytics

The CT-5322F/CT-5642F camera includes a rich set of video analytic functionality embedded in its firmware. The **Analytics** tab contains menus for defining the camera's field of view depth and detection rules, including region entrance, loitering, tripwire crossover, fence trespass, unattended baggage, stopped vehicle, and object removal.

In real-time, the camera sends notifications and alarms upon the occurrence of events. You can set customizable rules and criteria to define the perimeter, region, and what to detect. The camera's analytic software ensures a high probability of detection with an extremely low false alarm rate.
Use the **Analytics** tab to configure the following functions:

- Depth
- Rules
- Responses
- Scheduled Actions
- On-Screen Display
- Firmware
- Backup & Restore

Caution:

The camera is disarmed when configuring Analytics. Detection will not take place until the camera is manually re-armed from the **Home** screen.

Attention:

La caméra est désactivée lors de la configuration d'Analytics. La détection n'aura lieu qu'après que la caméra soit réactivée depuis l'écran ***Accueil****.*

Note:

For detailed instructions how to configure analytics, follow instructions in the *HTML Edition Units User's Guide*.

7.2.1 Configuring Depth Settings

The **Depth** screen enables you define the perspective of the scene being monitored. It is used to set human markers, ground guidelines, camera height, horizon, and advanced depth regions (such as hills, planes and fences), which create a virtual 3D model for measurement of distances and sizes from the perspective of the camera. The screen contains a wizard that facilitates configuring the depth settings.

Figure 26: Analytics > Depth Screen

There are two methods to configure depth settings:

- If you are performing setup by yourself, click the *Solo Setup* tab.
- If you are not performing setup alone, proceed to *Step 1: Ground & Height*.

> **Note:**
> It is possible to click the **Verification** tab to verify and apply settings at any time.

7.2.1.1 Solo Setup

The Solo Setup function enables you to install and setup the camera at a remote site without requiring another person's assistance. It is very useful and should be used even if you have another person's assistance. With this feature, you can:

- Move around within the camera's field of view.
- Use the camera to record a set of snapshots of the scene while the user is moving around the camera field of view. Creating the recording of the person in the FOV can be used to adjust settings without requiring another physical walk through the FOV.
- Use the recording of his movement to setup the depth by marking his height on the camera's field of view.

Follow the instructions in the **Solo Setup** tab to single-handedly setup the camera. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

To perform a solo setup

1. Click the **Solo Setup** tab. The Solo Setup keypad opens with the following control icons:

Icon	Function	Notes
	Start Recording	Starts recording and browses to destination folder where the clip will be saved
	Stop Recording	Stops recording
	Browse	Browses to the destination folder where clip is stored and loads the clip
	Play/Pause	Speed X1/X0
	Fast Forward	Speed X2, X4, X8, X16. Click to increase or decrease speed.
	Rewind	Speed -X2, -X4, -X8, -X16. Click to increase or decrease speed.

2. On the Solo Setup control keypad, click **Start Recording** to record a view in the camera's field of view.
3. Select a folder where to store the clip. Recording starts when the folder is selected.
4. Walk through various locations across the vertical axis of the camera's field of view in order to place ground and height markers and guidelines in the clip.
5. Click **Stop Recording** .
6. Proceed to the tab for **Step 1: Ground & Height**.
7. Click **Browse** to load the clip from the folder where it is saved.
8. Use the **Play** , **Pause** , **Fast Forward** , and **Rewind** buttons on the Solo Setup keypad to explore the clip. The status of the view is displayed on the bottom left side of the screen.

9. Click the round **Play** button on the control panel located to the left of the monitor to exit *Clip* mode and return to *Live* mode. The caption under the monitor changes from *Clip* to *Live.*

Figure 27: Analytics > Depth Control Panel

10. Proceed to the tabs for Steps 2-4 of the Depth Setup to complete the setup and apply settings.

> **Note:**
> At any time it is possible to click the **Verification** tab to verify and apply settings.

7.2.1.2 Configuring Ground and Height Settings

If you are not performing a solo setup, click the **Step 1: Ground & Height** tab.

To configure ground and height settings

1. Click the **Step 1: Ground & Height** tab. The **Step 1: Ground & Height** tab opens.

Figure 28: Analytics > Depth > Step 1: Ground & Height Tab

2. Follow the instructions on screen. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
3. Click **Apply** when finished or continue to the next step.

7.2.1.3 Configuring Camera and Horizon Settings

After completing Solo Setup or configuring ground and height settings, configure camera and horizon settings.

To configure camera and horizon settings

1. Click the **Step 2: Camera & Horizon** tab. The **Step 2: Camera & Horizon** tab opens.

Figure 29: Analytics > Depth > Step 2: Camera & Horizon Tab

2. Follow the on-screen instructions to configure camera and horizon settings. Refer to the HTML Edition Units User's Guide for detailed instructions on configuring these settings.
3. Click **Apply** when finished or continue to the next step.

7.2.1.4 Configuring Advanced Depth Region Settings

After configuring camera and horizon settings, configure Advanced Depth Region settings.

To configure advanced depth region settings

1. Click the **Step 3: Advanced Depth Regions** tab. The **Step 3: Advanced Depth Regions** tab opens.

Figure 30: Analytics > Depth > Step 3: Advanced Depth Regions Tab

2. Follow the on-screen instructions to configure advanced depth region settings. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
3. Click **Apply** when finished or continue to the next step.

7.2.1.5 Verification of Settings

After configuring advanced depth region settings, verify your settings.

To verify settings

1. Click the **Step 4: Verification** tab. The **Step 4: Verification** tab opens.

Figure 31: Analytics > Depth > Step 4: Verification Tab

2. Follow the on-screen instructions to verify settings. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.
3. Click **Apply** when finished.

7.2.2 Rules

The **Rules** tab enables you to define detection rules according to the type of detection you want to be notified about. By default, the *Human or vehicle enter region* rule is enabled.

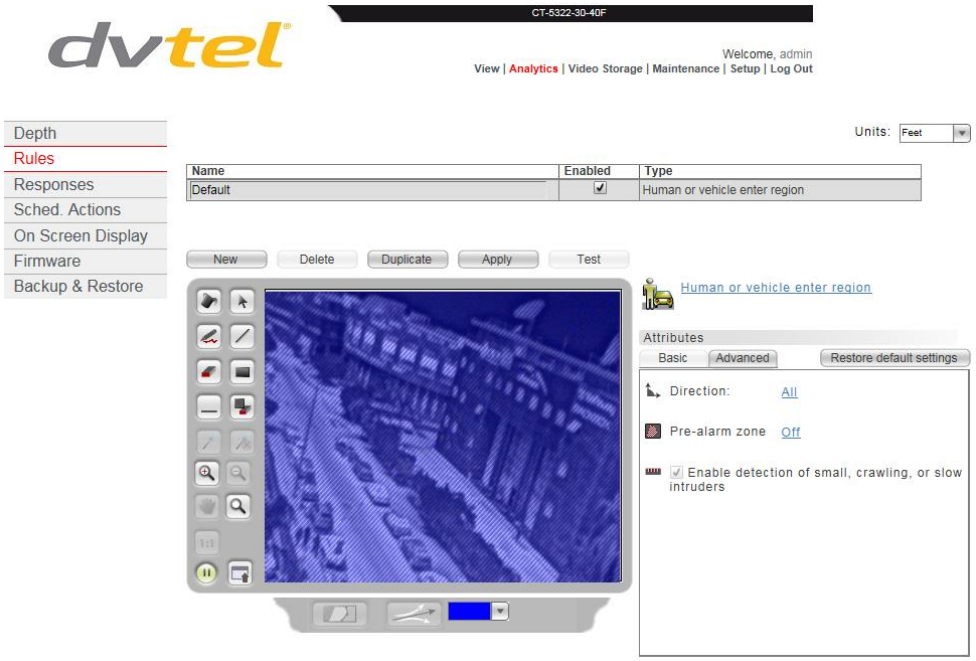


Figure 32: Analytics > Rules Screen

Detection occurs when one or more detection rules are active, the camera is in *Arm* mode, and the scenario on the video (scene) fits the detection criterion specified. When the conditions of a detection rule are met, an alarm is shown in which you can observe the detection and take the appropriate action. Rules are selected by clicking the **Attributes** tab. The **Attributes** tab includes **Basic** and **Advanced** settings tabs.

7.2.2.1 Basic Attributes Tab

The **Basic** tab displays minimal information for the rule.

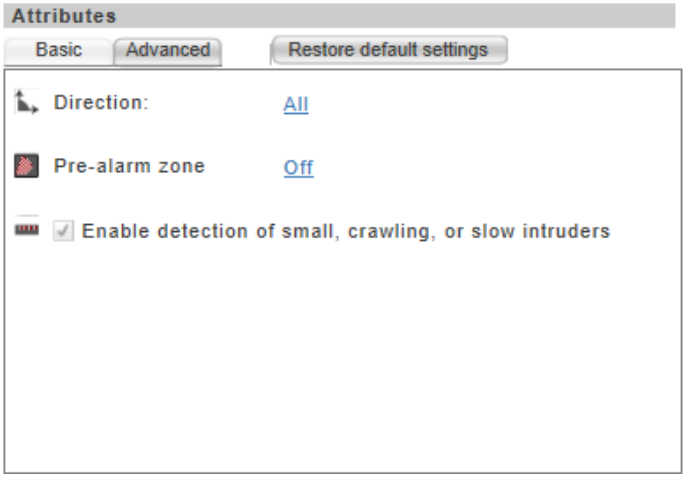


Figure 33: Analytics > Rules > Basic Attributes Tab

The analytic firmware includes an algorithm that improves the identification of people who are standing or moving upright in a scene. The system can detect sophisticated intruders (for example a camouflaged or crawling person), as well as enable the identification of upright people, which will reduce false alarms. This function is enabled or disabled by selecting *Enable detection of small, crawling or slow intruders*.

7.2.2.2 Advanced Attributes Tab

The **Advanced** tab displays additional information for the rule. Check *Show Human size* or *Show Vehicle size* if you want to display these sizes on-screen.

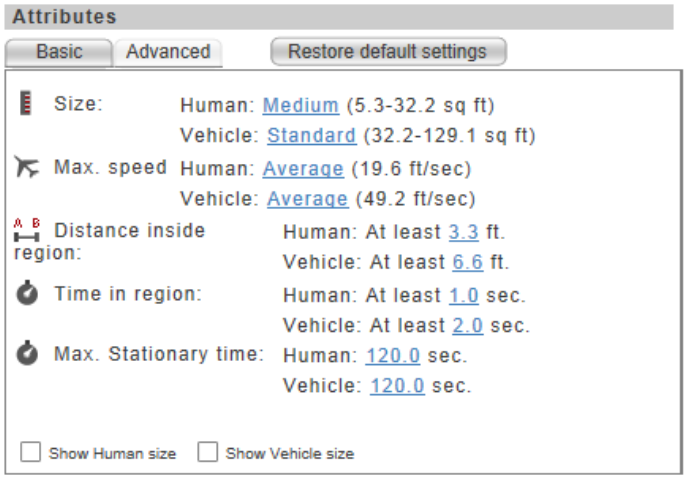


Figure 34: Analytics > Rules > Advanced Attributes Tab

Click **Restore default settings** to return to factory default settings. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

7.2.3 Responses

The camera's embedded event engine enables you to define a set of responses (automatic actions) for selected events and to perform actions (scheduled actions) at pre-defined times during a defined monitoring period. Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

Figure 35: Analytics > Responses Screen

Each automatic response definition includes the following three parameters: Triggering Event, Actions, and Schedule.

7.2.3.1 Triggering Event

A triggering event starts an automatic response. The *Triggering Event* tab enables you to define triggering events that initiate an automatic response. An automatic response is an action that is defined in the *Actions* tab and executed during the monitoring period defined in the *Schedule* tab.

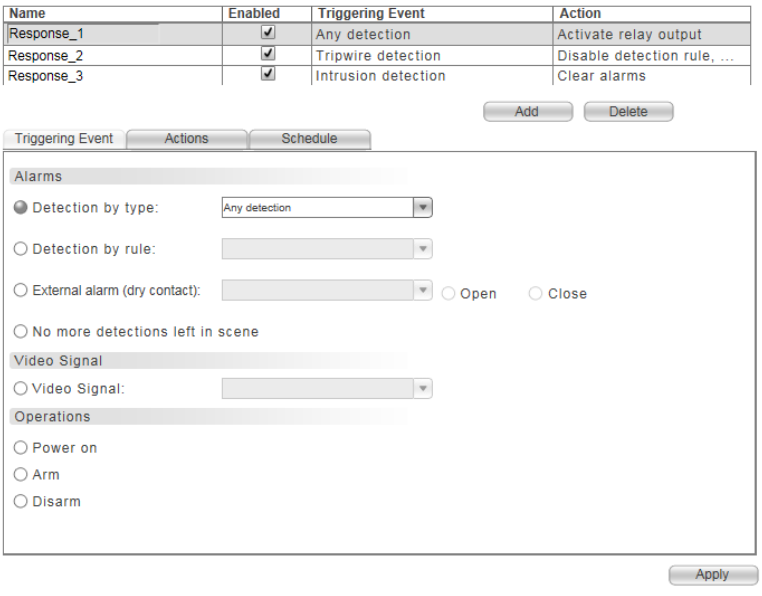


Figure 36: Triggering Event Tab

The *Triggering Event* tab includes the following fields:

Setting	Description
Detection by type	Triggers an automatic response in case the unit detects according to a detection rule matching the selected type: ▪ *Any detection* ▪ *Intrusion detection* ▪ *Vehicle Stopped* ▪ *Unattended Object* ▪ *Object Removed* ▪ *Tripwire detection* ▪ *Fence detection* ▪ *Loitering detection*
Detection by rule	Triggers an automatic response according to the name of the selected detection rule.
External alarm (dry contact)	Triggers an automatic response when the unit detects dry contact alarms received from connected alarm Inputs. Select *Alarm Input -1* or *Alarm Input -2*.
No more detections left in scene	Triggers an automatic response in case no detections are left in the scene.
Video Signal	Triggers an automatic response in case one of the following video signal status notifications occur: ▪ *Any Tamper* ▪ *Video Signal OK* ▪ *No Video Signal* ▪ *Low Video Signal* ▪ *Bad Video Signal*Camera Shift
Power On	Triggers an automatic response when the unit's power is turned on.
Arm	Triggers an automatic response when the unit's status is changed to arm.
Disarm	Triggers an automatic response when the unit's status is changed to disarm.

To create a Triggering Event

1. Select the *Triggering Event* tab.
2. Configure the fields described above. By default, the name *Response_1* is displayed in the *Name* column for the first action. To change the name, enter new text in the *Response_1* text box. By default, *Any detection* is displayed in the *Triggering Event* column and *Activate relay output* is displayed in the *Action* column. Changes to the Triggering Event and Action are made in the *Actions* tab and are displayed immediately in the table.
3. To enable the event, check *Enabled*.
4. Click **Apply**. The message *Configuration Saved* is displayed.
5. To create a new event, click **Add** at the top of the screen. Repeat steps 2-4.

7.2.3.2 Actions

An action is a step to perform in response to the occurrence of a triggering event. The *Actions* tab enables you to define the automatic response to perform at a scheduled time when the triggering event occurs during the monitoring schedule.

> **Warning:**
> The relay output can be used for automatic responses that are initiated without intervention from an outside user. Never use the relay output for automation that cannot be overridden or may cause damage, injury or loss of life. Because an ioi unit can automatically change the relay output state (NORMALLY OPEN or NORMALLY CLOSED) of devices controlled by the system, safety measures should be taken as a precaution.

To create an Action

1. After configuring the Triggering Event defined in the *Triggering Event* tab, select the *Actions* tab.
2. Click **Add** at the top of the tab. By default, the name *Response_1* is displayed in the *Name* column for the first action. By default, *Any detection* is displayed in the *Triggering Event* column and *Activate relay output* is displayed in the *Action* column. Changes to these settings are displayed in the table.

To configure the Actions tab

1. Select the *Actions* tab. The *Actions* tab is displayed.

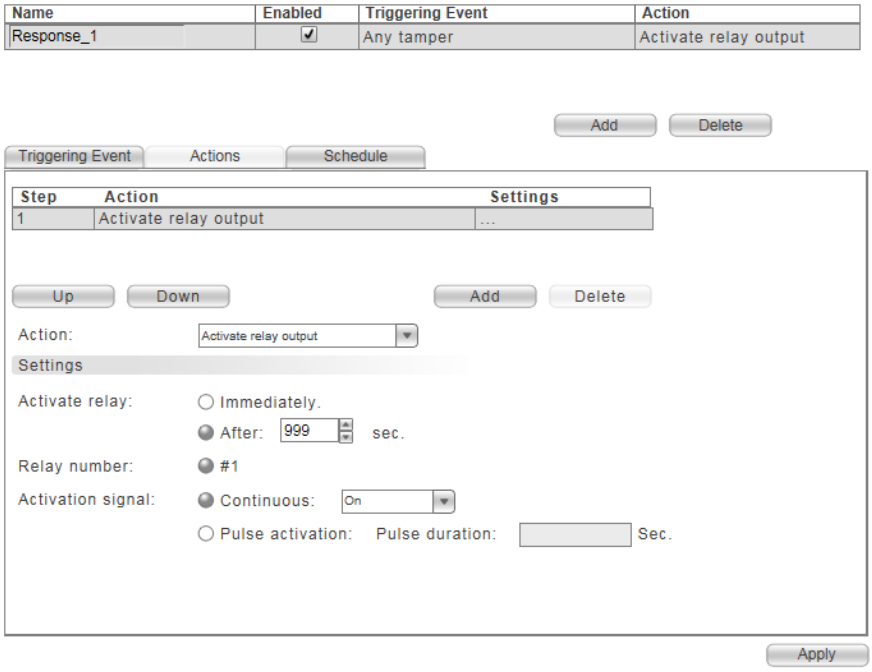


Figure 37: Actions Tab

2. From the Actions drop-down list, select the action to perform on event occurrence from the following options: Activate relay output, clear alarms, arm camera, disarm camera, enable detection rule, or disable detection rule. The configuration fields for each action are displayed in the *Settings* section of the tab.

The following actions are available:

Activate relay output

- In the *Activate relay* section, select one of the two options for when to activate the relay:
  - *Immediately*
  - *After x seconds* – Enter the number of seconds to wait enter in the text box.
- Select the Activation signal:
  - *Continuous*: Select *On* or *Off*
  - *Pulse activation:* In the *Pulse duration* field, enter the duration of the pulse in seconds. The range is from 1-65,535 seconds.

Clear alarms

- Select when you want to clear alarms:
  - *Immediately*
  - *After x seconds* – Enter the number of seconds to wait enter in the text box.

Arm/Disarm camera

- Select when you want the camera armed:
  - *Immediately*
  - *After x seconds* – Enter the number of seconds to wait enter in the text box.

Enable/Disable detection rule

- In the *Perform* section, select when you want a detection rule enabled or disabled:
  - *Immediately*
  - *After x seconds* – Enter the number of seconds to wait enter in the text box.
- The *Rule name* is according to the default.

3. If you want to add additional actions for this triggering event, click **Add** in the **Actions** tab. A new action is added to the *Action* list.
4. Configure the new action as described in steps 2 and 3.
5. To delete any of the actions for this triggering event, select the required action in the *Action* list and click **Delete**. The selected action is deleted.
6. To change the order in which you want to perform the actions, use the **Up** and **Down** buttons.
7. Click **Apply**.

7.2.3.3 Schedule

The *Schedule* tab enables you to configure a time schedule when the occurrence of triggering events should be monitored. Scheduled actions are actions performed on a specific date or on a recurring basis over a defined time period; on specific days or over a range of days; and at a specific time or at multiple specific times. The *Schedule* tab for automatic responses to events has the following fields:

Setting	Options	Description
Always		Defines continuous monitoring of triggering events.
Monitor event occurrence		Defines when a triggering event occurrence should be monitored.
	From	Selects the date on which the monitoring starts.
	To	Selects the date on which the monitoring ends.
	No end date	Used in conjunction with the *From* option, if the event monitoring is to run from the selected date with no end date.
	Weekdays	Select the days of the week on which the event monitoring is to take place.
	Between	Select the time of day during which the event monitoring is to take place. Time periods are entered in the format *hh:mm-hh:mm*, where the first time entry is the starting time and the second time entry is the finishing time. If multiple time ranges are required, the additional time ranges are separated by a space. For example, *hh:mm-hh:mm hh:mm-hh:mm.*

To configure the monitoring schedule

1. Select the *Schedule* tab. The *Schedule* tab is displayed.

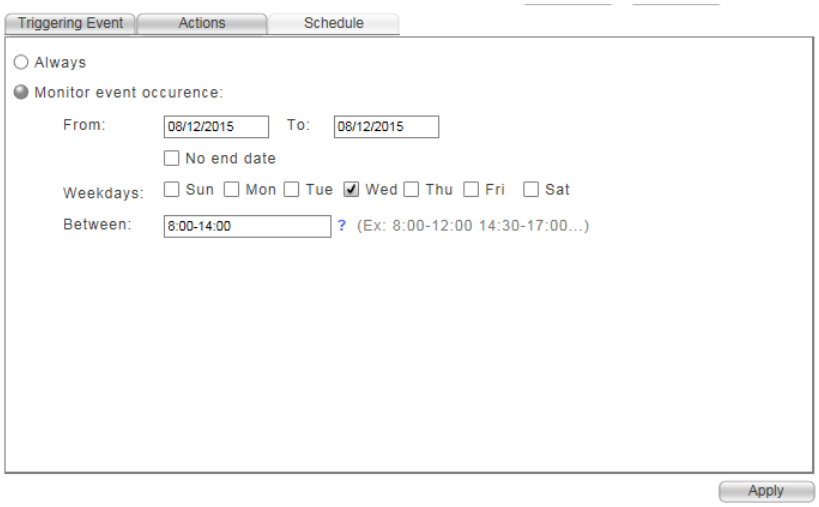


Figure 38: Schedule Tab

2. Select *Always* if you want the event to be continuously monitored.
3. If you selected *Always*, continue with step 5.

4. Select *Monitor event occurrence*.
5. Do one of the following:
   - In the *From* field, enter the date on which you want monitoring of the event to start
   - Click in the field and select the date from the calendar that is displayed
6. Do one of the following:
   - In the *To* field, enter the date on which you want monitoring of the event to end
   - Click in the field and select the date from the calendar that is displayed
7. If you want the event to be monitored with no end date, select *No end date*.
8. In the *Weekdays* field, select the day(s) on which you want the event monitored.
9. In the *Between* field, enter the time range during which you want the event monitored. Use the format *hh:mm-hh:mm*, where the first time entry is the starting time and the second time entry is the finishing time. If multiple time ranges are required, the additional time ranges are separated by a space. For example, *hh:mm-hh:mm hh:mm-hh:mm*.

   Note:
   Events that pass midnight and cross over into the next day must be configured twice: once for the time period till midnight and the other starting from midnight the next day.

10. Click **Apply**.

7.2.4 Sched. Actions (Scheduled Actions)

The **Responses** and **Sched. Actions** screens are similar, except that the **Sched. Actions** screen does not include the *Triggering Event* tab. See the Responses section above for details.

Each scheduled action includes the following two parameters:

- Actions – The actions to perform at the scheduled time.

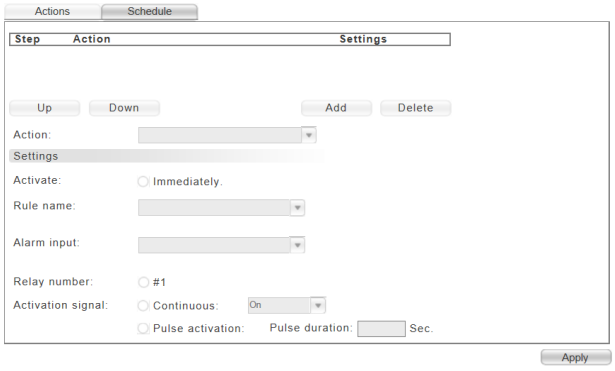


Figure 39: Sched. Actions > Actions Tab

- Schedule – When the actions must be performed.

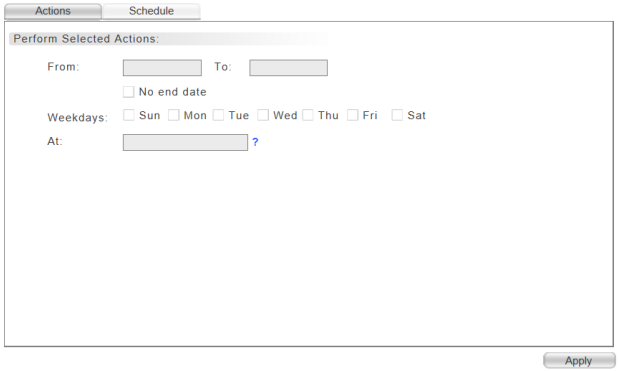


Figure 40: Sched. Actions > Schedule Tab

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

7.2.5 On Screen Display

The **On Screen Display** screen determines the information to be displayed on the video screen as an overlay on top of the video. The settings on this screen define the selection, alignment and color configuration of the various overlays that appear during normal monitoring, events and detection.

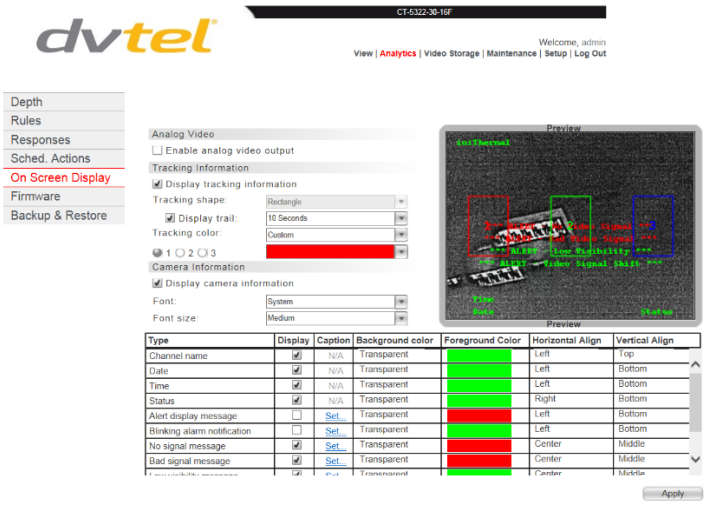


Figure 41: Analytics > On Screen Display Screen

The **On Screen Display** screen includes the following default settings:

- Enable analog video output
- Display tracking information
- Tracking shape: Rectangle
- Display trail enabled (10 seconds)
- Tracking color: Custom
- Radial button 1: Red
- Display camera information
- Font: Terminal
- Font size: Medium

In the table, select the settings that you want to configure.

- In the *Display* column, select the checkbox to display the display item.
- In the *Caption* column, click *Set* to change the name of the display item. You cannot change the names *Channel name, Date, Time* and *Status*.
- In the *Background color, Foreground color, Horizontal Align,* and *Vertical Align* columns, clicking a field opens a drop-down list. Select one of the options from the drop-down list.

Click **Apply** when finished.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

7.2.6 Analytic Firmware

The **Analytics > Firmware** screen displays the current analytics firmware version and enables you to update this firmware. It is also possible to configure advanced settings from this screen.

Note:
Analytics firmware is stored in a separate file than the camera system software. To view the camera system software version, see System > Software Version. To upgrade the camera system software version, see System > Software Upgrade.

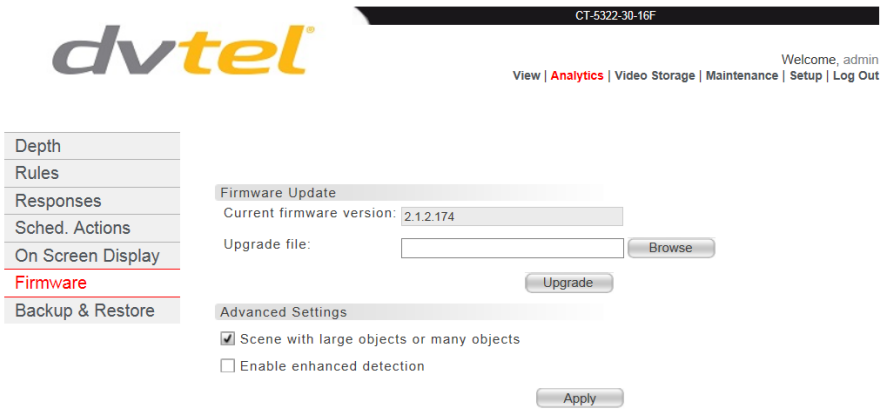


Figure 42: Analytics > Firmware Screen

To upgrade the analytic firmware

1. Click **Browse** to select the analytics firmware file.
2. Click **Upgrade**.
3. Click **Apply** when finished.

Note:
You must close and restart Internet Explorer in order to view the new firmware version.

The *Advanced Settings* section includes two settings, *Scene with large objects or many objects* and *Enable enhanced detection,* which are enabled by default.

7.2.6.1 Scenes with Large Objects or Many Objects

ioi Thermal offers enhanced detection in scenes where there are large or multiple objects, and there is movement in up to 80% of the frame. This function is enabled by default in the *Advanced Settings* area of the **Analytics > Firmware** screen. To deselect this function, uncheck the checkbox and click **Apply**.

7.2.6.2 Enable Enhanced Detection

The unit's analytic firmware includes an algorithm that improves the distance from which smaller objects are detected. This function is disabled by default. To enable this function, check the checkbox in the *Advanced Settings* area of the **Analytics > Firmware** screen. To deselect this function, uncheck the checkbox and click **Apply**.

7.2.7 Backup & Restore

The **Backup & Restore** screen enables you to create backup files of the unit's analytics settings and to restore them.

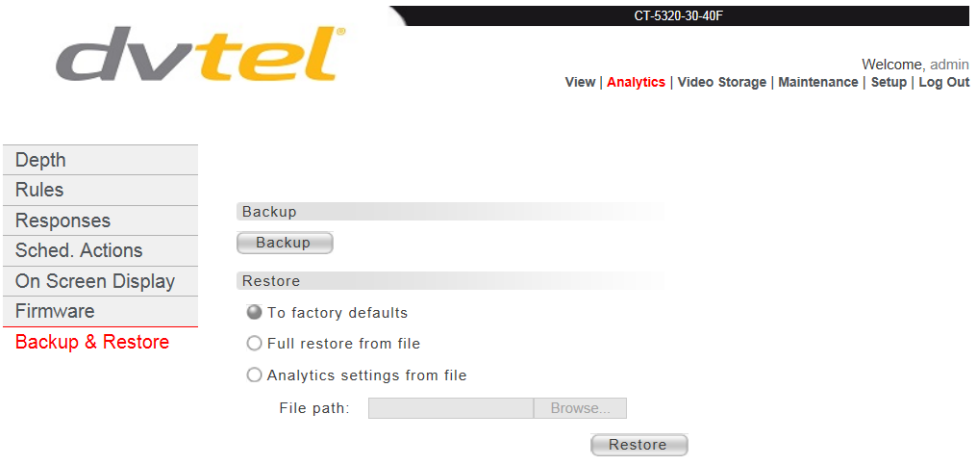


Figure 43: Analytics > Backup & Restore Screen

To back up the analytic firmware file

1. Click **Backup**.

To restore the analytic firmware file

1. Do one of the following:
   - To restore factory defaults, select *To factory defaults*.
   - To restore all defaults from a stored file, select *Full restore from file*, click **Browse** to locate the file path, then select the file.
   - To restore analytic settings from a stored file, select *Analytic settings from file*, click **Browse** to locate the file path, then select the file.
2. Click **Restore**.

Note:

Analytics firmware is stored in a separate file than the camera system software. To backup and restore the camera system software version, see Maintenance > System Update.

Refer to the *HTML Edition Units User's Guide* for detailed instructions on configuring these settings.

7.3 Video Storage

The **Video Storage** screen displays the date, size, time, and file name of the clips and images that are stored in 3.5GB of the camera's embedded flash memory.

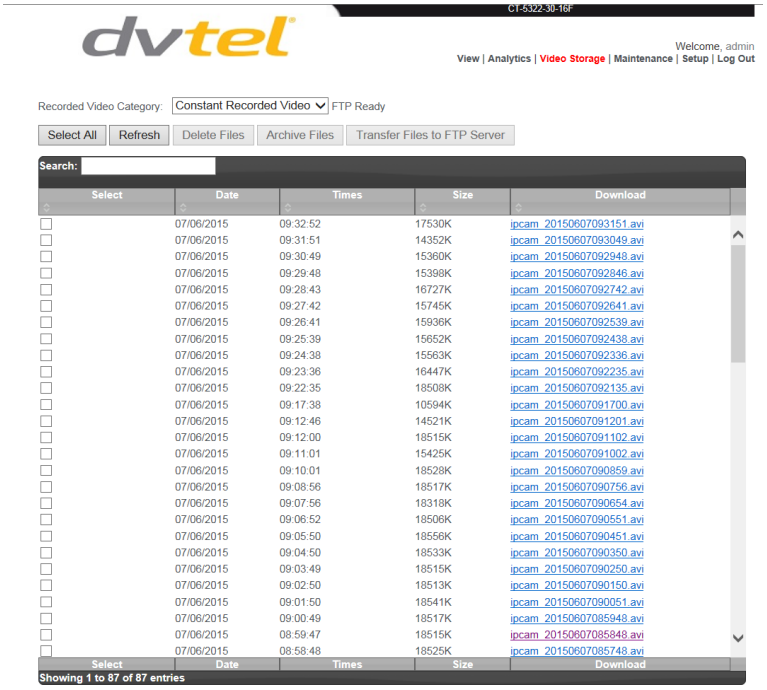


Figure 44: Video Storage Screen

From the *Recorded Video Category* drop-down list, select *Constant Recorded Video* or *Video Archive*. All videos are stored by default in the Constant Recorded Video folder. Files can be selected from this folder and moved to the Video Archive folder.

From the tabs, select the following options:

- *Select All* – Selects all files to delete, archive, or transfer via FTP. Click the relevant button to perform the desired action.
- *Refresh* – Refreshes the screen display.
- *Delete Files* – Deletes files checked in the *Select* column.
- *Archive Files* – Moves files checked in the *Select* column to the Video Archive folder.
- *Transfer Files to FTP Server* – Sends the files checked in the *Select* column via FTP to the remote server that is configured in the **Setup > Network > FTP Server** screen.

In the *Search* text box, enter the date, time, size or file name. The filtered results are displayed in the table.

Clips can be played back via the unit's web interface. Simply click on the file name and the clip is displayed in a pop-up window.

Figure 45: Video Storage Popup Viewer

7.4 Maintenance

The **Maintenance** tab provides access to the following screens:

- System Status (page 41)
- Restart Camera (page 42)
- Restore Factory Defaults (page 42)
- Format Local Storage (page 43)
- System Update (page 44)
- Camera Functions (page 44)
- Log (page 46)
- Copyright (page 47)

> **Note:**
> Only an Administrator has access to the **Maintenance** tab.

7.4.1 System Status

Clicking the **Maintenance** tab opens the **System Status** screen.

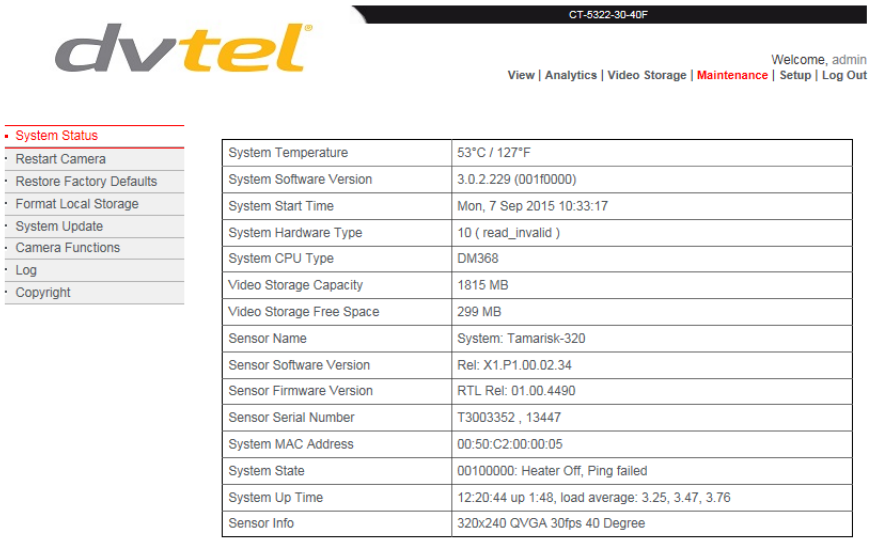


Figure 46: System Status Screen

The **System Status** screen provides the following information about the system and key system components:

- System — System temperature; system software version; system start time; system hardware type; system CPU type; system MAC address; system state; and system uptime.
- Video storage — Video storage capacity and video storage free space.
- Sensor — Sensor name; sensor software version; sensor firmware version; sensor serial number; and sensor info.

7.4.2 Restart Camera

The **Restart Camera** screen is used to reboot the camera.

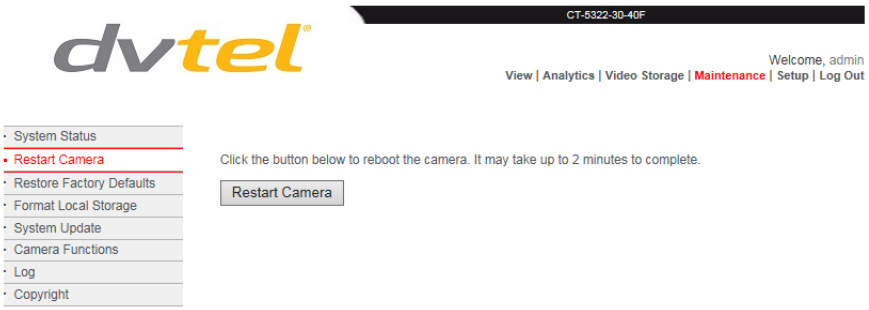


Figure 47: Restart Camera Screen

To restart the camera

1. From the sidebar, click **Restart Camera**.
2. Confirm the action in the popup window.The camera reboots within 120 seconds.
3. Refresh the screen or press the F5 key for the login prompt.

7.4.3 Restore Factory Defaults

The **Restore Factory Defaults** screen is used restore partial factory default settings, restore all factory default settings, and to restore analytics settings. From the sidebar, click **Restore Factory Defaults**.

Figure 48: Restore Factory Defaults Screen

To restore partial factory default settings

1. Click **Restore Partial Factory Defaults**. This restores the system and analytic settings.
2. Press the button again to confirm the action. The camera reboots to factory defaults, saving only the TCP/IP settings entered by the user. See TCP/IP Settings (page 48).

To restore all factory default settings

1. Click **Restore Factory Defaults**. This restores the system and analytic settings.
2. Press the button again to confirm the action. The camera reboots to all factory default settings.

> **Note:**
> The unit's IP address will revert to its original setting.

To restore analytic defaults

1. Click **Restore Analytics Defaults**. This restores the analytic settings only.
2. Press the button again to confirm the action. The camera reboots to restore all analytics default settings. The process may take three minutes to complete.

> **Caution:**
> In order to restore analytic defaults, from the **Analytics > Backup & Restore** screen, select *Analytics setting from file*.

7.4.4 Format Local Storage

Click **Format Storage** to format the unit's embedded flash memory. It is possible to store up to 3.5GB of constant video recordings and snapshots. The video includes analytic on-screen display information.

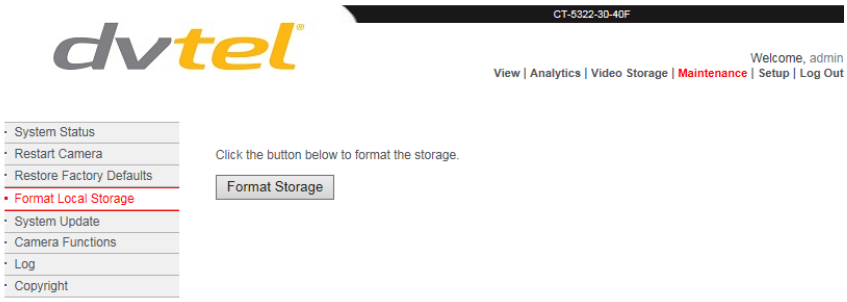


Figure 49: Format Local Storage Screen

7.4.5 System Update

The **System Update** screen is used to update the camera's firmware and to upload a new file of the camera's configuration parameters.

> **Note:**
> Only a qualified DVTEL technician should perform the camera configuration update.

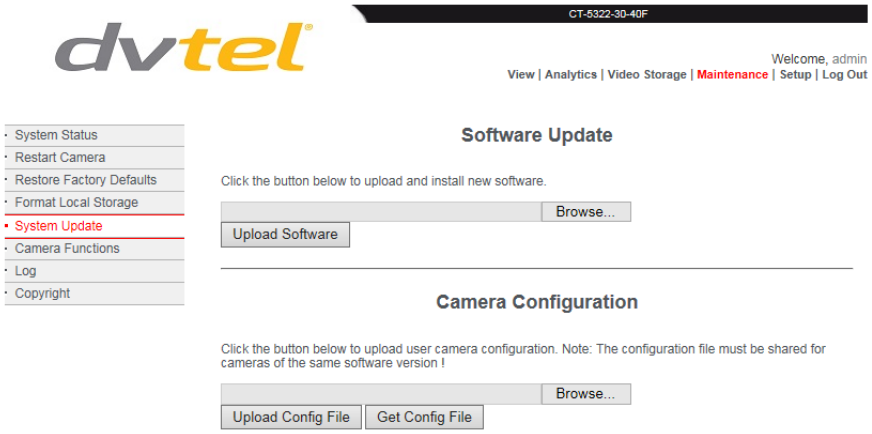


Figure 50: System Update Screen

To update the camera's software

1. Click **Browse** in order to locate the camera's firmware file.
2. Click **Upload Software**.
3. Confirm the action in the popup window. The file is uploaded.

> **Note:**
> Typical firmware update time is 20 minutes, but may take up to one hour, depending on network conditions.

To upload a configuration file

1. Click **Browse** in order to locate the configuration file.
2. Click **Upload Config File**.
3. Confirm the action in the popup window. The file is uploaded.

To retrieve a configuration file

1. Click **Browse** in order to locate the configuration file.
2. Click **Get Config File**.
3. Confirm the action in the popup window. The file is uploaded.

> **Note:**
> User configurations are not restored.

7.4.6 Camera Functions

The **Camera Functions** screen is used for the following functions:

- Display the camera temperature and heater duty cycle
- Automatically calibrate the camera at set intervals
- Enable/Disable constant recording

7.4.6.1 Heater Control

The **Camera Functions** screen opens on the **Heater Control** screen. The screen displays the camera temperature and heater duty cycle. By default, the camera heater is enabled.

Caution:

The camera must be powered by 802.3at PoE+, or by a 12-24VDC or 24VAC power supply with at least 20W output. An 802.3af PoE switch/injector does NOT have sufficient power to operate the camera.

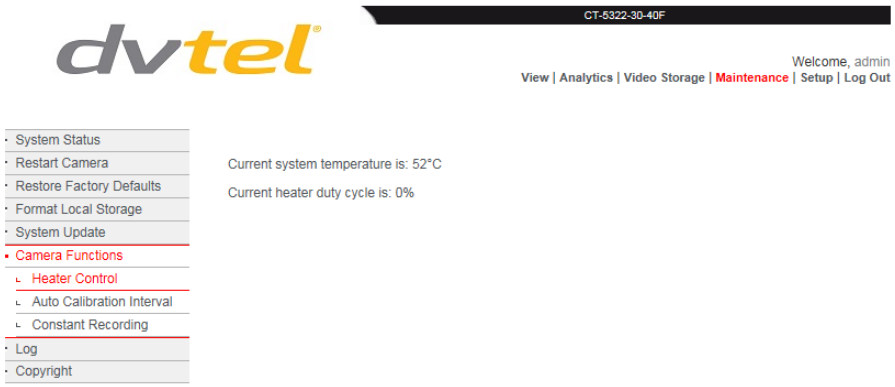


Figure 51: Heater Control Screen

7.4.6.2 Auto Calibration Interval

The **Auto Calibration Interval** screen enables the camera to automatically calibrate itself and perform non-uniformity correction (NUC) at frequent intervals. In addition, the camera will automatically perform NUC in case a temperature change is detected.

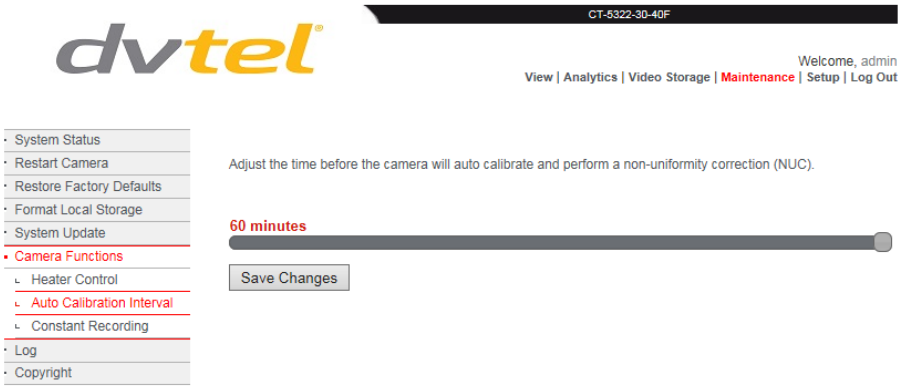


Figure 52: Auto Calibration Interval Screen

To set the Auto Calibration Interval

1. Choose the interval by using the slider. The NUC interval range is 5-60 minutes.
2. Click **Set**.
3. A popup window confirms the setting. The interval is set.

7.4.6.3 Enable/Disable Constant Recording

The **Constant Recording** screen is used to enable or disable constant recording. By default, Constant Recording is enabled.

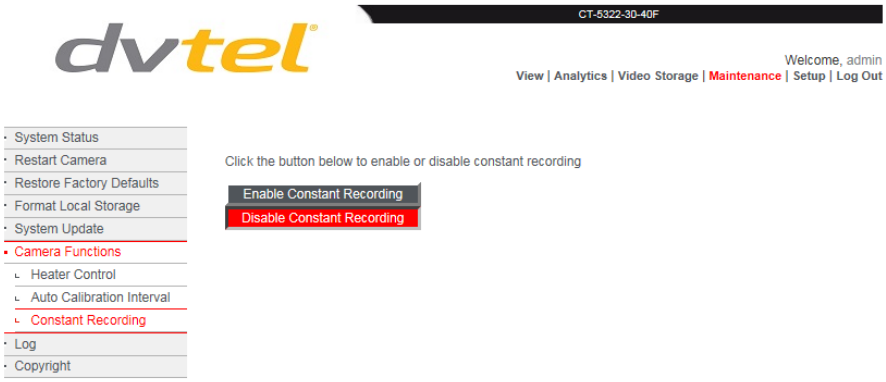


Figure 53: Constant Recording Screen

To enable constant recording

1. Click **Enable Constant Recording**. The camera starts to record continuously. By default, Constant Recording is disabled. When the camera's storage capacity is full, the camera will record over the oldest recordings.

To disable constant recording

1. Click **Disable Constant Recording.** The camera stops recording continuously.

7.4.6.4 Log

The **Log** screen is used for viewing and troubleshooting purposes. The logs may include camera start time, camera logout time, camera recording start time, and motion event time.

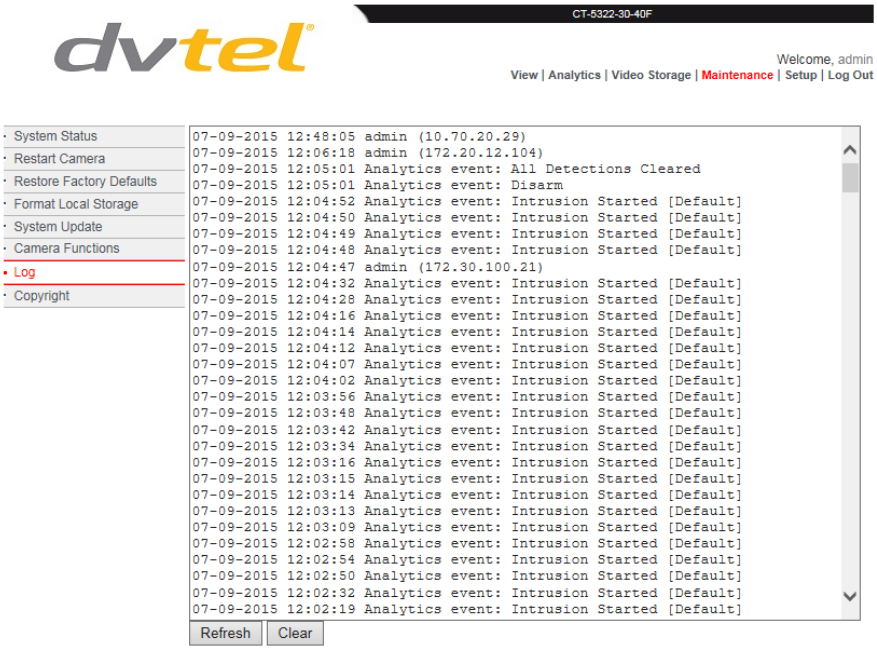


Figure 54: Log Screen

To view a log

1. Click **Refresh**. The updated log is displayed.

To clear the log

1. Click **Clear**. The log entries are erased.

7.4.6.5 Copyright

The **Copyright** screen displays the unit's copyright statement.

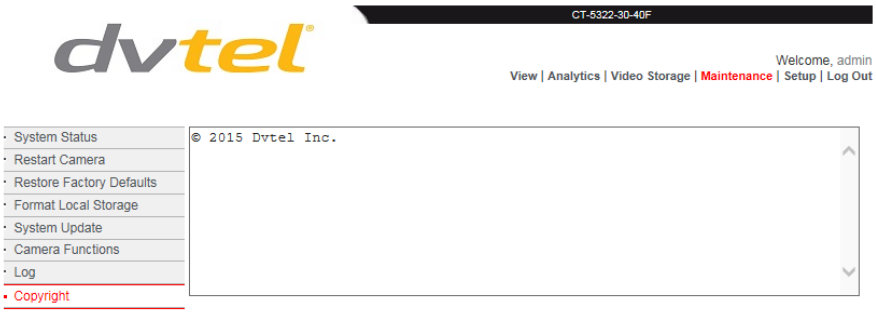


Figure 55: Copyright Screen

7.5 Setup

The **Setup** tab is used by Administrators to configure the following settings:

- Network settings (page 47)
- Account settings (page 53)
- Camera settings (page 53)

7.5.1 Configuring Network Settings

The **Network** tab is used to configure the following settings:

- TCP/IP Settings (page 48)
- FTP Server (page 49)
- Email (SMTP) Server (page 49)
- Ping Target (page 50)
- 802.1X (page 50)
- Zero Network Configuration (page 52)

7.5.1.1 TCP/IP Settings

The ioi CT-5322F/CT-5642F Fixed Thermal Analytic IP camera uses the TCP/IP protocol to configure network settings in order to communicate over an Internet Protocol (IP) network.

To configure TCP/IP settings

1. From the **Setup > Network** screen, select **TCP/IP settings**. The **TCP/IP Settings** screen opens.

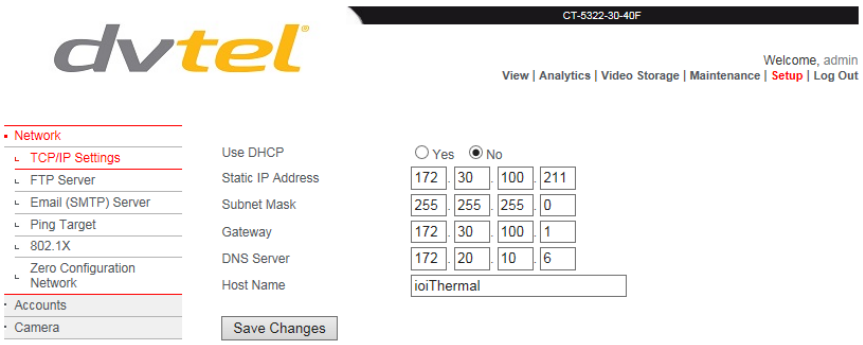


Figure 56: TCP/IP Settings Screen

2. Configure the following settings:

Network Setting	Description
Use DHCP	Select *Yes* if your network includes a DHCP server for dynamic allocation of IP addresses. Select *No* to manually enter the IP address and enter the IP address for the camera.
Static IP Address	Enter the Static IP address for the camera.
Subnet Mask	If you selected *No*, enter the subnet mask for the IP camera. Use the same value that is configured for the PCs on your network.
Gateway	If you selected *No*, enter the gateway for the IP camera. Use the same value that is configured for the PCs on your network.
DNS Server	Enter the IP address of the DNS server that is used in your network. Use the same value that is used for the PCs on your LAN.
Host Name	The default name is CT-5xxx-y-zF, where: • xxx is the model number by focal plane array size (320 or 640) • y is the frame rate in FPS • z is the lens FOV and camera type is F (fixed) You can enter a friendly name for the camera.

3. Click **Save Changes**.

7.5.1.2 FTP Server

An FTP server may be used for transferring recorded video images and files.

To configure FTP server settings

1. From the **Setup > Network** screen, select **FTP Server**. The **FTP Server** screen opens.

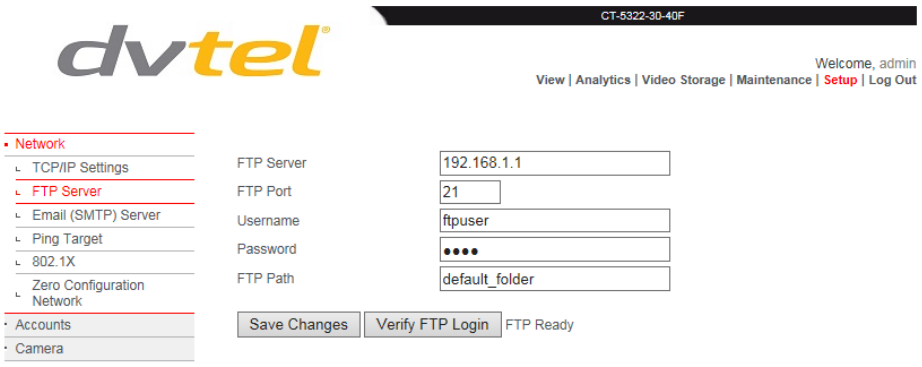


Figure 57: FTP Server Screen

2. Configure the following settings:

Network Setting	Description
FTP Server	Enter the FTP Server IP address.
FTP Port	Enter the FTP port number used on the network. The default is 21.
Username	Enter the username to access the FTP Server.
Password	Enter the password to access the FTP Server.
FTP Path	Enter the FTP Path name, which is the default folder for storing the FTP server configuration files.

3. Click **Save Changes** to save the settings.
4. Click **Verify FTP Login** to verify that the settings are correct. If they are correct, the message “FTP Ready” is displayed next to the button.

7.5.1.3 Email (SMTP) Server

This function is not supported in this version.

7.5.1.4 Ping Target

The **Ping Target** screen is used to verify that the camera is online by sending a ping (packet) to another device on the same network. If the other device is is online, the Ping Status "Success" is displayed. If the other device is not online, the Ping Status is indicated as "Failed".

To ping a device

1. From the **Setup > Network** screen, select **Ping Target**. The **Ping Target** screen opens.

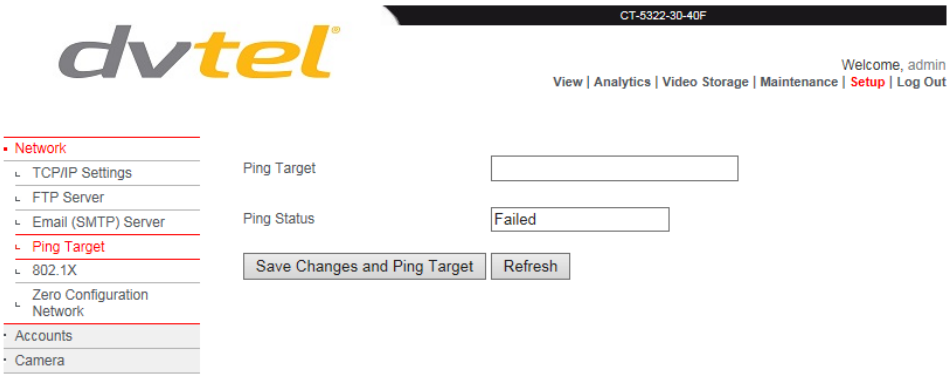


Figure 58: Ping Target Screen

2. Configure the following settings:

Network Setting	Description
Ping Target	Enter the IP address of another device (the target) on the same network.
Ping Status	Indicates whether the target device is online.

3. Click **Save Changes and Ping Target** to save the settings and send a ping to the target device.
4. Click **Refresh** to update the settings.

7.5.1.5 802.1X

802.1X is an IEEE standard that provides a framework for the encapsulation of Extensible Authentication Protocol (EAP) messages on an Ethernet network. 802.1X is typically administered on the port of an Ethernet switch. It is used to authenticate the credentials (such as username/password or digital certificate) of a device that wants to access a network. The settings require a RADIUS or equivalent server to be configured in the network in order to authenticate the camera.

The CT-5322F/CT-5642F supports the following 802.1X authentication methods:

- EAP-MD5
- EAP-GTC
- EAP-MSCHAPv2
- EAP-TTLS
- PEAPv0-MSCHAPv2

These EAP methods can provide a secure authentication mechanism and negotiate a secure private key between the camera and the network authentication server.

To authenticate the camera with 802.1X

1. From the **Setup > Network** screen, select **802.1X**. The **802.1X** screen opens.

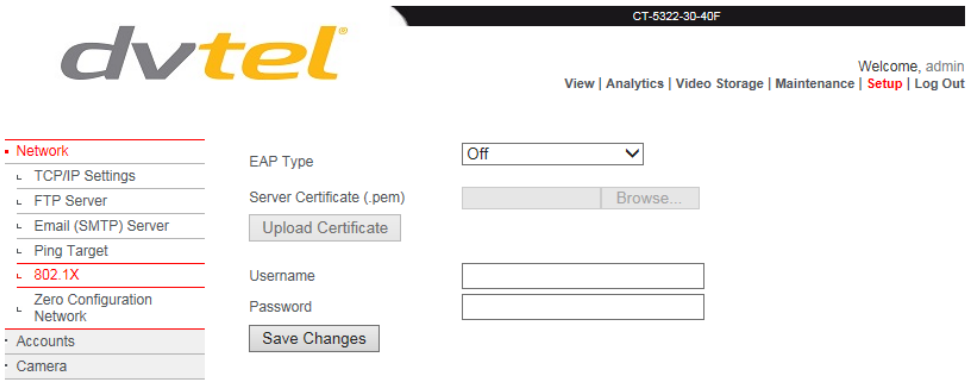


Figure 59: 802.1X Screen

2. Configure the following settings:

Network Setting	Description
EAP Type	From the drop-down list, select one of the following authentication options: • Off – Do not use authentication • EAP-MD5 • EAP-GTC • EAP-MSCHAPv2 • EAP-TTLS • PEAPv0-MSCHAPv2 **Note:** EAP-MSCHAPv2, EAP-TTLS, and PEAPv0-MSCHAPv2 require a certificate for authentication.
Server Certificate	Click **Browse** to locate the digital certificate (`*.pem` file) used to authenticate the camera on the authentication server.
Username	Enter the username to unlock the private key in the camera certificate.
Password	Enter the password to unlock the private key in the camera certificate.

3. Click **Upload Certificate** to upload the digital certificate to the camera.
4. Click **Save Changes** to save the username and password.

7.5.1.6 Zero Network Configuration

Zero Network Configuration (zeroconf) is a methodology that automatically creates an IP-based computer network without requiring manual operator intervention or special configuration servers. When zeroconf is disabled, a network administrator must use servers, such as DHCP and DNS servers, to configure the unit's network settings, or manually configure each device's network settings. By default, zeroconf is disabled.

To enable Zero Network Configuration

1. From the **Setup > Network** screen, select **Zero Network Configuration**. The **Zero Network Configuration** screen opens.

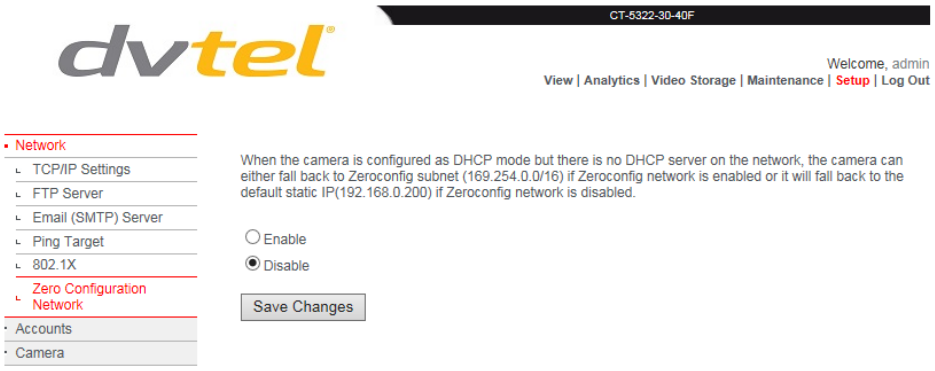


Figure 60: Zero Network Configuration Screen

2. Configure the following settings:

Network Setting	Description
Enable	Enables the camera to revert to a Zeroconfig subnet (169.254.x.y) when DHCP mode is configured and there is no DHCP server on the network or if the DHCP server fails. This applies to Windows networks using Automatic Private IP Addressing (APIPA). **Note:** 1. APIPA allocates IP addresses in the range 169.254.0.1 to 169.254.255.254. 2. This function does not work if the camera is assigned a static IP address.
Disable	Sets the camera to the default static IP address (192.168.0.200) if there is no DHCP server on the network. This is the default setting.

3. Click **Save Changes** to save the setting.

Note:

If there is no DHCP server on your network, do one of the following:

1. If you select *Enable,* set 169.254.255.255 as the IP address for the client PC. Set the PC mask as 255.255.0.0. Then set up the camera with a static IP address.
2. If you select *Disable*, set 192.168.0.11 as the IP for the client PC. Set the PC mask as 255.255.0.0. Then set up the camera with a static IP address.

7.5.2 Configuring Account Settings

The **Account** tab is used to enter the username, password, and user class for each user. It is possible to add, update or delete user accounts. In addition, it is possible to enable ONVIF security from this screen.

To configure account settings

1. From the **Setup** screen, select **Accounts**. The **Accounts** screen opens.

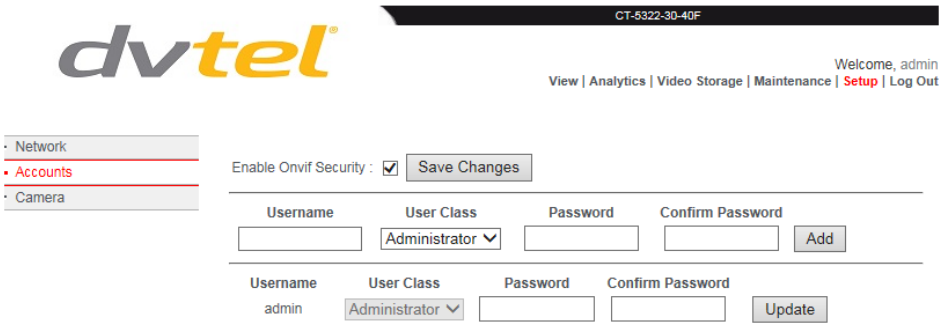


Figure 61: Accounts Screen

2. Select the *Enable Onvif Security* checkbox if you want to use the ONVIF Advanced Security Service for keys and certificates management (keystore) and TLS server configuration for ONVIF devices.
3. Enter the following settings for each user:

Setting	Description
Username	Enter the username to access the camera.
User Class	The user class determines which screens the user can access. Select a class from the drop-down list: • Administrator — can access all screens. • Operator — can access the **View** and **Video Storage** screens. • Viewer — can access the **View** screen, but cannot change parameters.
Password	Enter the password to access the camera.
Confirm Password	Re-enter the password.

4. Click **Add** to add the user.
5. Click **Update** to change the settings.
6. Click **Delete** to delete the user.
7. Click **Save Changes** to save the settings.

7.5.3 Configuring Camera Settings

The **Camera** tab is used to configure the following settings:

- Date and Time (page 54)
- Video Streaming (page 55)
- Video Settings (page 56)
- Analog Video Output (page 57)

7.5.3.1 Date and Time Settings

The **Date and Time** screen is used to set the current date and time.

To configure date and time settings

1. From the **Setup > Camera** screen, select **Date and Time**. The **Date and Time** screen opens.

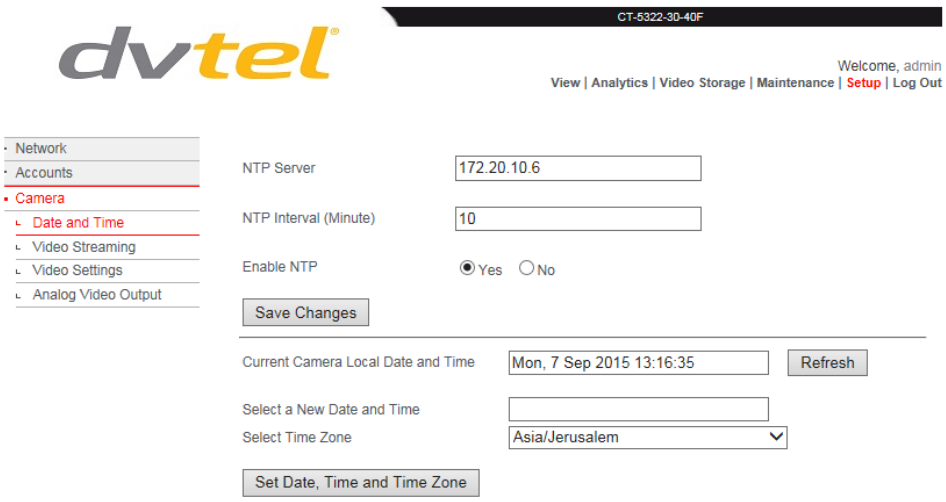


Figure 62: Date and Time Screen

2. To configure the date and time settings, enter the following information:

Field	Description
NTP Server	Enter the address for the NTP server.
NTP Interval (Minute)	Enter the number of minutes between requests for the time service to synchronize with the unit.
Enable NTP	Select *Yes* or *No*.

3. Click **Save Changes**.
4. To configure the current date, time and timezone settings, enter the following information:

Field	Description
Current Camera Local Date and Time	This field displays the current local date and time. Click **Refresh** to update the date and time.
Select a New Date and Time	Click the text box to enter the date and time to manually override the NTP settings.
Select Time Zone	From the drop-down list, select the local time zone. Daylight Savings Time is enabled automatically by default when you select your time zone. If you are located in an area that does not observe Daylight Savings Time, look for your region in the list.

5. Click **Refresh Time** to update the current data and time settings.
6. Click **Set Date, Time and Time Zone** to save the settings.

> **Note:**
> NTP must be disabled in order to save changes.

7.5.3.2 Video Streaming Settings

The **Video Streaming** screen is used to configure H.264 and MJPEG streaming settings.

To configure video streaming settings

1. From the **Setup > Camera** screen, select **Video Streaming**. The **Video Streaming** screen opens.

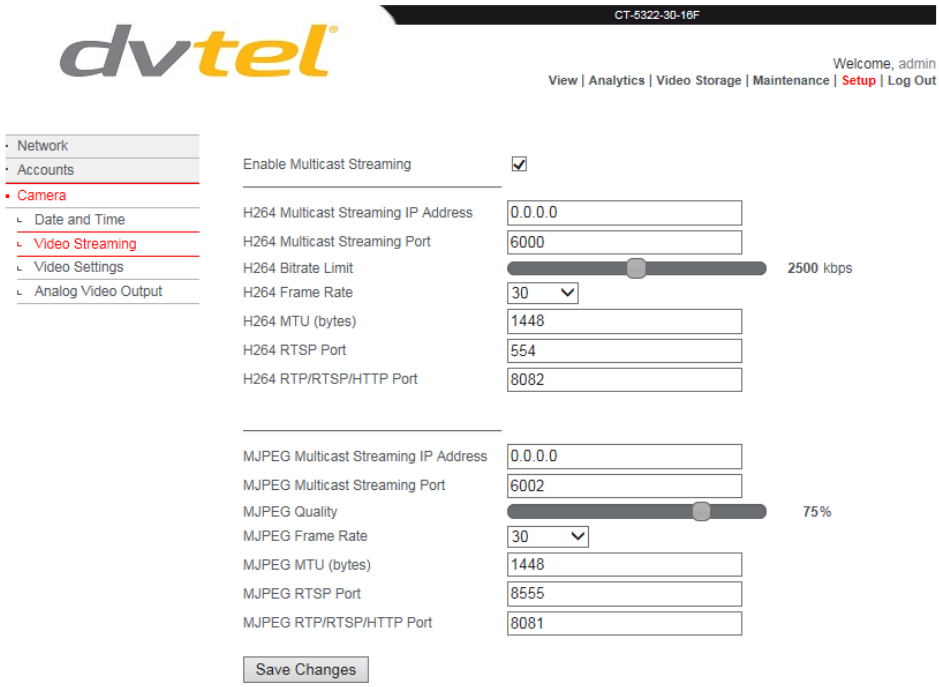


Figure 63: Video Streaming Screen

2. To configure the video streaming settings, enter the following information:

Field	Description
Enable Multicast Streaming	Check this box to select multicast streaming. By default, multicast streaming is enabled.
H264 Multicast Streaming IP Address	Enter the multicast streaming address. Valid range for multicast IP address is between 224.0.0.0 and 239.255.255.255. Typical multicast IP address is 239.x.y.z
H264 Multicast Streaming Port	Enter the multicast streaming port number. Port number can vary between 1 and 65535. Default value is 6000.
H264 Bitrate Limit	Use the slider to select the maximum bit rate for H.264 video. The available range is between 64Kbps to 5000Kbps.
H264 Frame Rate	From the drop-down list, select a frame rate from 5-9 FPS or CT-5XXX-9-YYF or 5-30F FPS for CT-5XXX-30-YYF.
H264 MTU (bytes)	Enter the MTU setting. When data is encrypted on a network, additional bytes are added to a data packet, which slows real-time transmission time. In order to improve real-time video performance, the MTU (Maximum Transmission Unit) size can be defined by setting the RTP packet size (in bytes) on the **Setup > Network > RTP Length** screen. The maximum value = 1448; the minimum value = 800. The default is 1448.
H264 RTSP Port	Enables setting a custom port for RTSP streaming. The default port is 554.

Field	Description
H264 RTP/RTSP/ HTTP Port	Enter the port used for H.264 RTP/RTSP/HTTP communication.
MJPEG Multicast Streaming IP Address	Enter the multicast streaming address. Valid range for multicast IP address is between 224.0.0.0 and 239.255.255.255. Typical multicast IP address is 239.x.y.z
MJPEG Multicast Streaming Port	Enter the multicast streaming port number. Port number can vary between 1 and 65535. Default value is 6001.
MJPEG Quality	Select the appropriate bit rate for MJPEG video by using the slider. The available range is 1% to 98%.
MJPEG Frame Rate	From the drop-down list, select a frame rate from 1-9 FPS or CT-5XXX-9-YYF or 1-30F FPS for CT-5XXX-30-YYF.
MJPEG MTU (bytes)	Enter the MTU setting. See H264 MTU explanation above.
MJPEG RTSP Port	Enables setting a custom port for RTSP streaming.
MJPEG RTP/RTSP/ HTTP Port	Enter the port number used for MJPEG RTP/RTSP/ HTTP port communication.

3. Click **Save Changes**.

7.5.3.3 Video Settings

The **Video Settings** screen is used to define the color and details you want to display in the On-Screen Display.

To configure video settings

1. From the **Setup > Camera** screen, select **Video Settings**. The **Video Settings** screen opens.

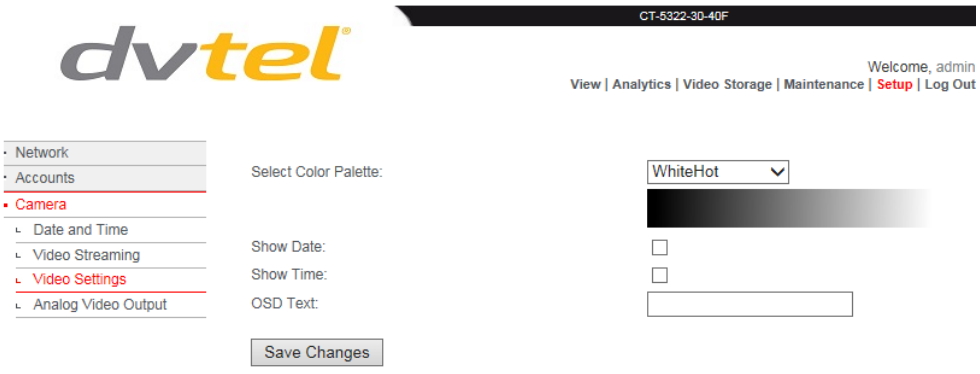


Figure 64: Video Settings Screen

2. From the *Select Color Palette* drop-down list, select the color or effect for viewing the thermal image.
3. To display today's date, check the *Show Date* checkbox.
4. To display the current time, check the *Show Time* checkbox.
5. To display text in the On-Screen Display, enter the text in the *OSD Text* text box.
6. Click **Save Changes**.

7.5.3.4 Analog Video Output Settings

The **Analog Video Output** screen is used to set the TV standard (PAL or NTSC). The default is PAL.

> **Caution:**
> Changing the TV standard resets the camera, which results in restoring analytic settings to default.

To configure the analog video output

1. From the **Setup > Camera** screen, select **Analog Video Output**. The **Analog Video Output** screen opens.

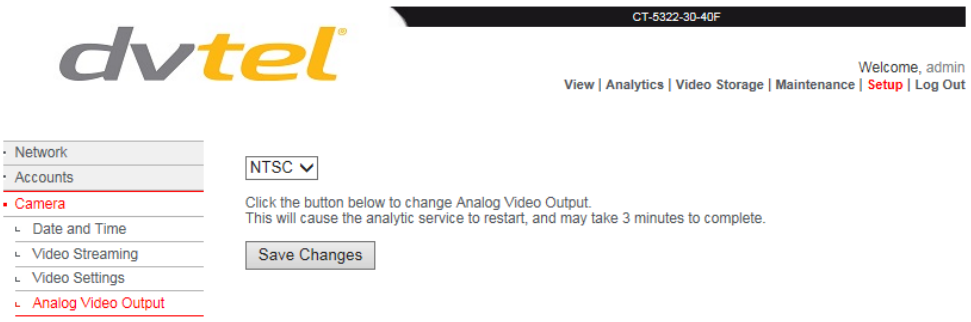


Figure 65: Analog Video Output Screen

2. From the drop-down list, select *PAL* or *NTSC*.
3. Click **Save Changes**.

7.6 Log Out

To log out of the camera, click **Log Out** on the navigation bar or at the bottom of the screen. All of the five main menus also have the **Log Out** button at the bottom of the screen.

Appendix

The appendix contains the following sections:

- Technical Specifications (page 60)
- CT-5322F/CT-5642F Mounting Accessories (page 62)
- Troubleshooting (page 70)
- Acronyms and Abbreviations (page 73)

A.1. Technical Specifications

Following are the CT-5322F/CT-5642F technical specifications:

Focal Plane Array						
Sensor Type		Uncooled Vanadium Oxide Microbolometer				
Array Format	CT-5322F	320 x 240 (QVGA)				
	CT-5642F	640 x 480 (VGA)				
Pixel Pitch		17µm or less				
Spectral Band		8-14µm (LWIR)				
Sensitivity (NEDT) @ f/1.0		< 50mK at f/1.0				
Optics						
Lens		Athermalized Fixed Focus				
Lens Options	CT-5322F	Horizontal Field of View (HFOV), Lens Aperture, and Effective Focal Length				
		6° f/1.2 50mm	9° f/1.2 35mm	16° f/1.1 19mm	24° f/1.2 13mm	40° f/1.2 7.5mm
	CT-5642F	12° f/1.2 50mm	18° f/1.2 35mm	25° f/1.2 25mm	37° f/1.25 16.7mm	44° f/1.4 14.25mm
Video						
Frame Rate	H.264	**9 FPS Models**			**30 FPS Models**	
		Configurable 5-9 FPS			Configurable 5-30 FPS	
	MJPEG	Configurable 1-9 FPS			Configurable 1-30 FPS	
Format		Analog: NTSC/PAL IP: H264/MJPEG				
Gain/Level Control		Automatic/Freeze/ICE (Image Contrast Enhancement) for superior performance				
Contrast		Manually adjustable				
Brightness		Manually adjustable				
Image Polarity		White Hot, Black Hot				
Hardware						
Embedded Memory		3.5GB for continuous recordings and snapshots				

Network	
Ethernet	1 x 10/100Mbps RJ45 interface (IEEE 802.3/802.3u)
Services and Protocols	RTP, RTSP, TCP/IP, UDP/IP, DHCP, FTP, HTTP, HTTPS, SMTP, DNS, SNTP, UPnP, ONVIF 12.14 and Profile S (December 2014)
Video Streaming	H.264, MJPEG
Alarms/Commands	TCP/IP, HTTP, ONVIF
Password Levels	Administrator, Operator, and Viewer with Password Protection
Security	IEEE 802.1X, ONVIF Advanced Security Service
Operating System	Windows 7, Windows 8, Windows 8.1
Internet Browser	Internet Explorer 8, 9, 10, or 11 (32-bit version)
I/O Interface	
Alarm Input	2 x dry contacts
Relay Output	1 x relay output (rated load 0.3A@ 30VDC)
Power Source	
Voltage	12VDC, 2 amps; 24VDC, 1 amp, 24VAC, or IEEE 802.3at (PoE+)
Power Consumption	<20W with or without built-in heater
Mechanical	
Dimensions (mm/inches)	292 x 104 x 95 mm/11.5 x 4.1 x 3.74” (W x H x D)
Weight	<1.2kg (2.6 lbs.)
Enclosure	Tamper-Resistant IP66
Environmental Specifications	
Operating Temperature	-40° to 60°C (-40° to 140°F)
Storage Temperature	-50° to 75°C (-58° to 167°F)
Operating Humidity	5% to 95% (non-condensing)
Certifications	
Safety	CE (IEC 60065 7th Edition/AM1/AM2, EN60065:2002/A1:2006/ A2:2010/A11:2008/A12:2011); UL 60065 7th Edition; CAN/CSA-C22.2 No. 60065-03, 1st Edition+A1:2006+A2:2012; IEC 60068-2-6, FC, ET 51; IEC 60529, IPX6
Electromagnetic Interference (EMC)	CE (EN 61000-6-4:2007+A1:20011; EN 61000-6-2:2005); FCC 47 CFR Part 15 (FCC 15.107:2015 and FCC 15.109:2015), Subpart B, Class A; ICES-003:2012 Class A; CISPR 22:2009+A1:2010 Class A; VCCI:2014-04 Class A; RCM
Environmental	RoHS Directive 2011/65/EU and 2002/95/EC; WEEE. Dispose of this equipment as electronic waste.

A.2.Accessing a Remote Unit over the Web

ioi Thermal cameras enable IP access to a camera that does not have built-in IP capability. Furthermore, it is possible to remotely access a unit that is located behind a firewall at a remote site. ioi Thermal does this by using port forwarding, which enables three functions:

1. Transmitting videos over remote networks.
2. Remote configuration of the unit over the web. The web setup supports login, all setup functions, and video display configuration.
3. Remote configuration of the video analytics module.

Port forwarding maps and enables communication between an external IP address (accessible over the Internet) and an internal IP address (assigned to a unit on a private network located behind a firewall/router with or without a firewall), which is not directly accessible over the Internet. ioi Thermal cameras enable IP access to a camera that does not have built-in IP capability.

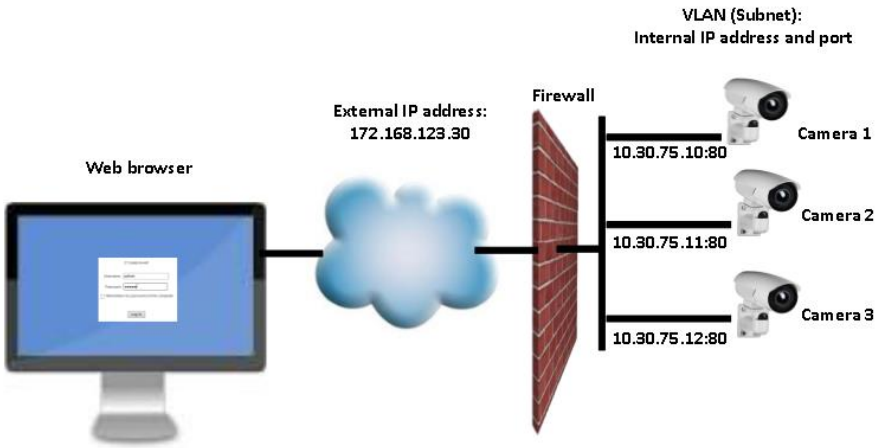


Figure 66: Remote Access System

The following port forwarding table displays an example of the mapping between the external IP address/port and the internal IP address/port:

Camera #	External IP Address:Port Number	Internal IP Address:Port Number
Camera 1	172.168.123.30:180	10.30.75.10:80
Camera 1	172.168.123.30:181	10.30.75.10:8080
Camera 1	172.168.123.30:182	10.30.75.10:554
Camera 2	172.168.123.30:280	10.30.75.11:80
Camera 2	172.168.123.30:281	10.30.75.11:8080
Camera 2	172.168.123.30:282	10.30.75.11:554
Camera 3	172.168.123.30:380	10.30.75.12:80
Camera 3	172.168.123.30:381	10.30.75.12:8080
Camera 3	172.168.123.30:382	10.30.75.12:554

Note:

The user must configure three consecutive ports for each camera in the router port forwarding table.

- First port is used to forward port 80 (HTTP)
- Second port is used to forward port 8080
- Third port is used to forward port 554 (used by the video stream)

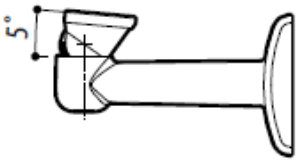
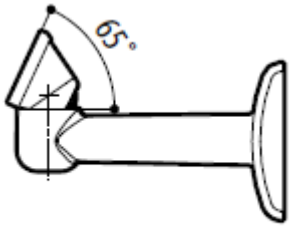
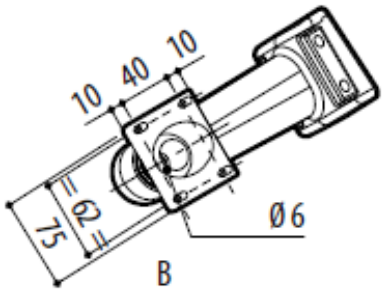
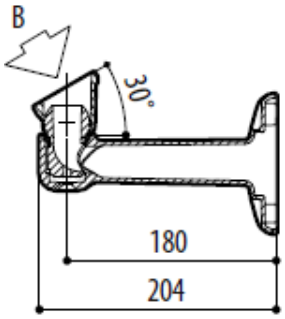
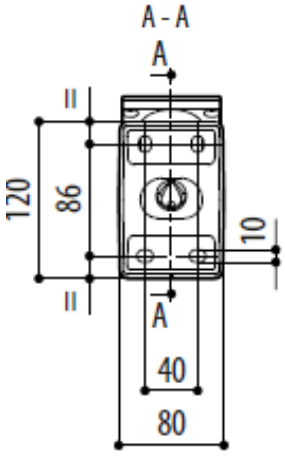
To access a remote device

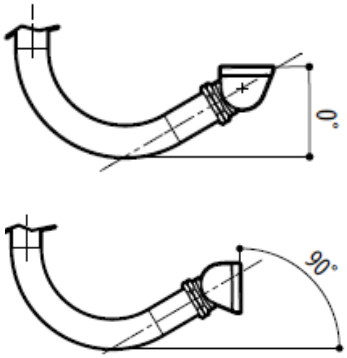
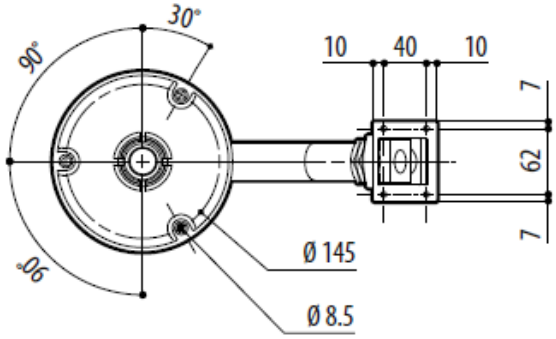
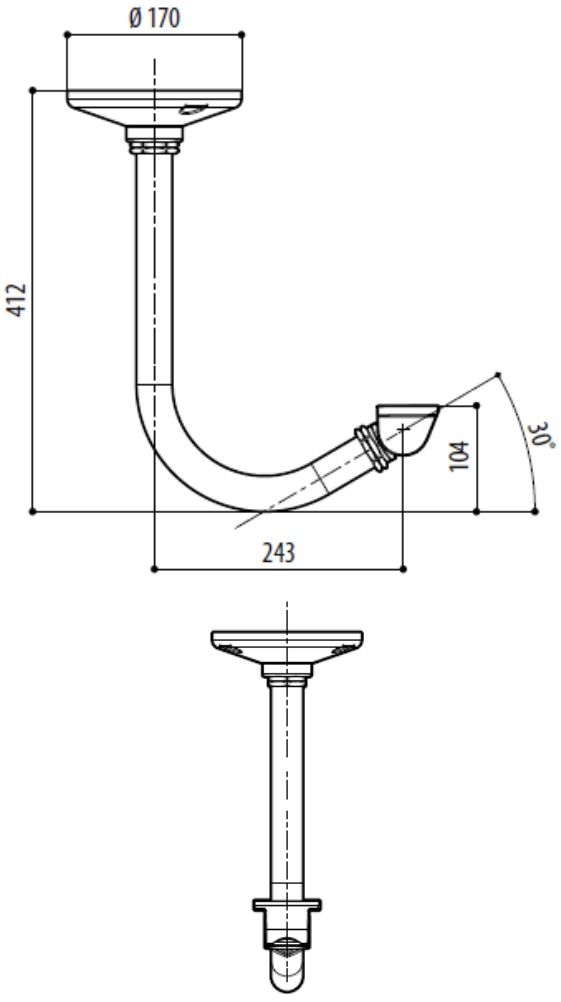
1. On the client PC browser, enter “http://[NAT external IP]:[port 80 forwarded port]” For each unit. For example, http://172.168.123.30:180. The camera’s **Login** window opens. See Figure 20: Login Window (page 17).
2. Login to the camera.
3. Enter the unit’s **Setup** screen.
4. Perform the required action.

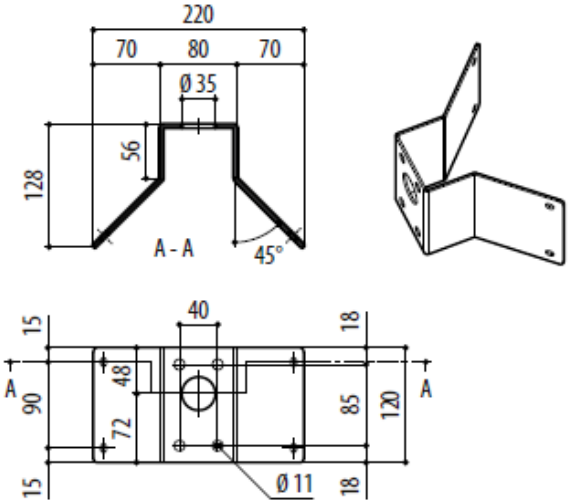
A.3.CT-5322F/CT-5642F Mounting Accessories

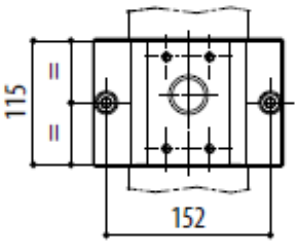
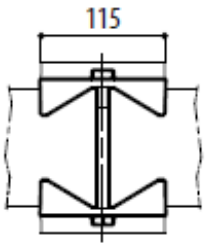
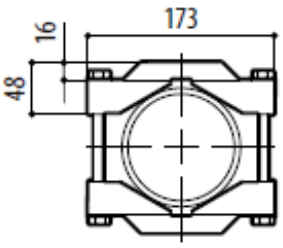
The following mounting accessories are available from DVTEL for installation of your ioi Thermal fixed camera. For more information on available options, contact your DVTEL sales representative or visit www.DVTEL.com to request details on where to get the accessories you need.

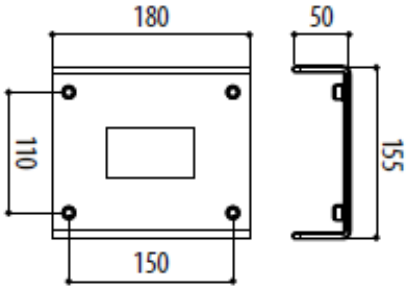
All products are for indoor/outdoor installation and are epoxy polyester powder-painted in RAL9002 color.
All products are supplied with housing screws. Housing position adjustment is made with only one bolt.
All measurements are in millimeters, 1:10 scale.

Name	Image	Description
CT-WALL-00	   MAXIMUM INCLINATION	Wall bracket with joint, including an internal cable channel, for vandal-proof protection. For IP55 protection, cut a hole in the supplied sheath of 2mm (0.08”) less than the cable diameter and connect to the existing hole of the bracket. Material: Die-cast aluminum Unit weight: 0.6kg (1 lb. 5 oz.) Load rating: 25kg (55 lbs.) Length: 204mm (8 in.)   

Name	Image	Description
CT-CEILING-00	 MAXIMUM INCLINATION 	Ceiling bracket with an internal cable channel. It combines easy position adjustment and vandal-proof protection. Suitable for housings with cable management. Material: Extrusion and die-cast aluminum Unit weight: 1.3kg (2 lbs. 14 oz.) Load rating: 15kg (33 lbs.) Length: 412mm (16.2 in.)  

Name	Image	Description
CT-CORNER-00		Kit including CT-WALL-00 mount and corner adapter. It allows the cable to pass internally through a slot to connect to the CT-WALL-00 bracket. Constructed from steel. For corner installation. Material: Stainless steel corner and die-cast aluminum mount Unit weight: corner 1kg (2 lbs. 3 oz.); mount 0.6kg (1 lb. 5 oz.) Load rating: 30kg (66 lbs.) Weight: 1kg (2.2 lbs.) 
CT-ADAPTER-00		Reinforcing wall plate adaptor. It allows the cable to pass internally through a slot to connect to the CT-WALL-00 bracket. For wall installation. Material: Die-cast aluminum Unit weight: 0.7kg (1 lb. 8 oz.) Load rating: 50kg (110 lbs.) Weight: 0.7kg (1.5 lbs.)

Name	Image	Description
CT-POLE-01		Kit including CT-WALL-00 mount and reinforced supporting pole clamp. It allows the cable to pass internally through a slot to connect to the CT-WALL-00 bracket. For pole installation. Material: Die-cast aluminum clamp with stainless steel tie-rods Unit weight: pole clamp 0.9kg (2 lbs.); mount 0.6kg (1 lb. 5 oz.) Load rating: 30kg (66 lbs.) Pole: Ø 65 - 110mm (2.5 - 4.3 in.) Weight: 0.9kg (2 lbs.)   

Name	Image	Description
CT-POLE-02	 	Kit including pole mount adapter, CT-WALL-00 and CT-ADAPTER-00. Material: Die-cast aluminum clamp with stainless steel tie-rods Unit weight: pole clamp 2.8kg (6 lbs. 3 oz.); mount 0.6kg (1 lb. 5 oz.); pole adapter 0.7kg (1 lb. 8 oz.) Pole diameter: 80-150mm- 3.14” to 5.9”.
CT-POLE-03	 	Kit including pole adapter for CT-WALL-00 and CT-ADAPTER-00. Material: Die-cast aluminum clamp with steel pole adaptor Unit weight: pole clamp 1.5kg (3 lbs. 5 oz.); mount 0.6kg (1 lb. 5 oz.); pole adapter 0.7kg (1 lb. 8 oz.) Max load: 25kg (55 lbs.) Pole diameter: 210-225mm (8.2”to 8.85”) Weight: 1.1kg (2.4 lbs.) 

A.4.Troubleshooting

This section provides useful information and remedies for common situations where problems may be encountered.

Problem	Possible Solution
No network connection	**Hardware issues**: • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the LED on the Ethernet (RJ-45) connector on the power connection panel of the unit is on. • Confirm that the network cables are not damaged and replace if necessary. **IP Address issues**: • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet.Contact your IT administrator to get the IP address of the camera.
How do I find IP address of my unit?	• Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	• Disconnect the unit's Ethernet 10/100 port or turn the power to unit off, and then ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the PoE+ switch/port and ensure that the port is working OK. Ensure that the switch ports provide the necessary power. The camera requires a minimum of 13 watts of power.
The unit IP address is in use by another computer (collision)	• Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).
Cannot login to the camera	• Check the login user ID of the user or admin. • Check the login password of the user or admin.

Problem	Possible Solution
No video image displayed on the main menu or the view menu of the web Interface	• Reset the browser security settings to the default value. Go to **Tools > Options**. • Check that the correct port was configured. The default port is 554.
No analog output video signal	• Make sure the analog video out is enabled on the unit/channel. • Check that the video cables are securely connected between the unit's VIDEO OUT BNC connector and the analog video source. • Check that the connection is made to the correct VIDEO OUT connector of the analog video source. • Confirm that the camera has power. • Check the cables for damage and replace as needed. • Check that the monitor screen has been refreshed, especially after firmware upgrade of the camera. Also clear the browser cache.
Bad output video quality	• Check the source video signal quality by connecting an analog monitor to the video source. If video quality is acceptable, connect the video source to the unit. • Check that the cables are connected securely. This includes junction boxes and amplifier that may be used. • Check that the camera settings are correct on the camera and in the unit.. • Check that the camera lens is clean and unobstructed. • Check that the analog video signal is not being degraded due impedance caused by lengthy or worn cable, numerous connectors, ground loops interference, and so on. • Check that the cable length is within specification.
Streaming video image is hanging (stopped)	• Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.

Problem	Possible Solution
Alarm inputs are not working	• Check the unit settings to confirm that the alarm input is enabled. Refer to the *HTML Edition Units User's Guide* for details. • Check that a proper rule for an alarm input event has been defined in the unit. Refer to the *HTML Edition Units User's Guide* for details. • Check that the alarm input (dry contact close/open) is being provided by the connected device. • Check that the unit is communicating through the network. • Check that the alarm input wires are connected securely. • Check that the alarm wires are paired in the terminal block in the right positions and according to requirements.
Relay outputs are not working	• Check the unit settings to confirm that the relay output is enabled. Refer to the *HTML Edition Units User's Guide* for details. • Check that a proper rule for activating a relay output has been defined in the unit or activate it manually. Refer to the *HTML Edition Units User's Guide* for details. • Check the relay output wires are connected securely. • Check that the relay output wires are paired in the terminal block according to requirements and that one wire is connected to the common. • Check that the NO or NC matches the system NORMALLY OPEN or NORMALLY CLOSED configuration.

A.5.Acronyms and Abbreviations

Abbreviation	Description
802.1X	Network Access Control Port based standard
AGC	Automatic Gain Control
DHCP	Dynamic Host Control Protocol
EULA	End User Licensing Agreement
FTP	File Transfer Protocol
H.264	Video Compression Standard
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
MJPEG	Motion Joint Photographic Experts Group
NEDT	Noise Equivalent Delta Temperature
NTP	Network Time Protocol
ONVIF	Open Network Video Interface Forum
ROI	Region of Interest
RTP	Realtime Transport Protocol
RTSP	Realtime Streaming Protocol.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play Protocol

Contacting DVTEL

To contact us, write us at info@dvtel.com or contact your local office.

CORPORATE HEADQUARTERS **DVTEL, Inc.** 65 Challenger Road Ridgefield Park, NJ 07660 USA Tel: 201.368.9700 Fax: 201.368.2615 Order Fax: 201.712.0343 info@dvtel.com	**ASIA PACIFIC REGION** **DVTEL** 111 North Bridge Road, #27-01 Peninsula Plaza Singapore 079098 Tel: +65 6389 1815 Fax: +65 6491 5660 info.apac@dvtel.com
ANZ AND THE PACIFIC ISLANDS **DVTEL** 37 Victoria Street Henley Beach, SA 5022 Australia Tel: +61 8 8235 9211 Fax: +61 8 8235 9255 Mobile: +61 419 850 166 info.anz@dvtel.com	**EMEA** **DVTEL UK Ltd.** 7 Lancaster Court, Coronation Road High Wycombe HP12 3TD England Tel: +44 (0) 1494 430240 Fax: +44 (0) 1494 446928 info.uk@dvtel.com
INDIA AND SAARC, GULF REGION **DVTEL India Pvt., Ltd**. 303, SSR Corporate Park Mathura Road Faridabad 121002 Haryana, India Tel: +91 (129) 431 5031 Fax: +91 (129) 431 5033 info.asia@dvtel.com	**CENTRAL AND LATIN AMERICA** **DVTEL Mexico S.A.P.I. de C.V.** Felipe Villanueva No. 10 Col. Guadalupe Inn México, D.F. 01020 México Tel: +5255 5580 5618 Fax: +52 55 8503 4299 info.cala@dvtel.com
DVTEL NORTH ASIA 2404, 24/F, World-Wide House 19 Des Voeux Road Central Hong Kong Tel: +852 3667 9295 Mobile: +852 9479 4195 info.northasia@dvtel.com	**DVTEL北亞地區** 香港中環德輔道中19號 環球大廈2404室 電話: +852 3667 9295 手提: +852 9479 4195 電郵: info.northasia@dvtel.com

To request the latest versions of firmware and software or to download other product-related documents, visit http://www.dvtel.com/support. If you have obtained a login, go to our support gateway. For assistance, email us at support@dvtel.com or phone 1-888-DVTEL77.